KPMG Klynveld EDP Audit

90/1
winter 1989/1990

COMPACT

MONSTEREXEMPLAAR NIET MEENEMEN

Computer en Accountant

BETALINGSVERKEER

COMPUTER EN ACCOUNTANT

Inhoudsopgave blz.

Nummer 50 **Winter 1989/1990**
ISSN 0920-1645

VAN DE REDACTIE VAN COMPACT

Het verschijnen van deze Compact nummer 50 betekent niet alleen het tiende lustrum, maar ook de afsluiting van een tijdperk en het begin van een nieuwe.

Compact is oorspronkelijk opgezet als een intern periodiek dat vooral bedoeld was voor ondersteuning van de controlepraktijk. Er bleek in de loop van de 16 jaren dat Compact is verschenen steeds meer belangstelling te bestaan bij relaties, hetgeen heeft geresulteerd in een groot aantal externe abonnees.

In verband met het toegenomen belang van de externe abonnees heeft de redactie van Compact besloten om de interne status van het blad met ingang van het lentenummer 1990 te beëindigen. Als voortvloeisel van deze beslissing is met Samsom-uitgeverijen een contract getekend, waarvan de belangrijkste bepalingen zijn:
- de redactieverantwoordelijkheid berust bij een door KPMG Klynveld EDP Audit te benoemen redactie;
- Samsom regelt dat het tijdschrift verkrijgbaar zal zijn voor iedereen die daarin is geïnteresseerd;
- bestaande externe abonnees zullen het blad gratis blijven ontvangen, met dien verstande dat het aantal exemplaren dat ter beschikking wordt gesteld, wordt beperkt.

Nieuwe abonnementen kunnen worden opgegeven aan Samsom:
Samsom Bedrijfsinformatie
T.a.v. de heer H.B. Plas
Postbus 4
2400 MA ALPHEN AAN DEN RIJN

De voorliggende Compact is dus de laatste in de "oude stijl" en is als themanummer geheel gewijd aan het betalingsverkeer. In zeven artikelen, geschreven door deskundigen binnen en buiten KPMG Klynveld EDP Audit, worden uiteenlopende aspecten van het betalingsverkeer belicht.

Een betaling is in het Nederlands taalgebruik de voldoening van een geldschuld. In de rechtstaal is de betekenis ruimer: het verrichten van een verschuldigde prestatie.
Geld kan worden gedefinieerd naar de functies die het kan vervullen: ruilmiddel, rekeneenheid en spaarmiddel. In het betalingsverkeer gaat het om eerstgenoemde functie.
Naar de vorm kan onderscheid worden gemaakt tussen chartaal en giraal geld. Giraal geld is te beschouwen als een abstracte vorm van het concrete chartale geld (charta = document) en bestaat uit tegoeden in rekening-courant bij bankinstellingen die direct opeisbaar zijn in chartaal geld.
Giraal geld kan ook worden gebruikt voor het verrichten van betalingen, door overboeking naar een andere rekening-courant.
Het girale geld, in de functie van ruilmiddel, staat in dit themanummer centraal.

Het girale betalingsverkeer, dat in de Middeleeuwen is ontstaan, heeft in de twingstigste eeuw een enorme vlucht genomen.
Net zoals het chartale geld het edelmetaal als ruilmiddel heeft verdrongen, lijkt nu het girale geld de plaats in te gaan nemen van het chartale geld, zeker gelet op de opkomst van de betaalautomaten. Hoewel sommigen hierin wellicht een manifestatie zien van de wet van Gresham ("bad money always drives out good money"), is de redactie van mening dat deze ontwikkelingen op haar eigen merites moeten worden beoordeeld en dat er geen reden is voor pessimisme, wel voor behoedzaamheid.

In dit themanummer zal met name aandacht worden besteed aan de technologische ontwikkelingen rond het girale betalingsverkeer en de (beveiligings)risico's die deze oproepen.

Het openingsartikel, van de hand van de heer S. Lelieveldt, gaat in op de vraag hoe de banksector door gebruikmaking van informatietechnologie concurrentievoordelen kan behalen.

In een bijdrage van de heer M. Groesz wordt het elektronische betalingsverkeer geplaatst in het bredere kader van Electronic Data Interchange (EDI) en wordt (kort) stilgestaan bij de consequenties van EDI voor de accountantscontrole van de jaarrekening.

Een belangrijk deel van het geautomatiseerde betalingsverkeer wordt verzorgd door de Postbank. De heren C.P. Aland en A.H. Kuijlaars, beiden werkzaam bij de IAD van de Postbank, lichten het plan "Produktie-Innovatie" toe om het verwerkingsproces te vernieuwen. Speciaal wordt stilgestaan bij de aspecten van interne controle en beveiliging.

De beveiligingsaspecten van het geautomatiseerde girale betalingsverkeer en de wenselijkheid en mogelijkheid van standaardisatie, staan centraal in het artikel van de heer A. Hemelaar, adjunct-directeur bij de BankGiroCentrale.

Werd in de twee voorgaande artikelen de infrastructuur van de verwerking van de betalingen toegelicht, in de bijdrage van de heer H.C. Kocks wordt ingegaan op de risico's die bestaan bij de organisatie die de betalingsopdrachten aanlevert, in het bijzonder het frauderisico.

De risico's die zich voordoen bij het elektronisch verzenden van berichten en betalingsopdrachten en de mogelijkheden van cryptografische beveiligingstechnieken om deze risico's te beperken, vormen het onderwerp van het artikel van de heer T.P. de Vries.

In het slotartikel, van de heren P.M. Knuvers en G.H.M. Meijer, worden de aspecten van interne controle en beveiliging bij betalingen via het netwerk van S.W.I.F.T. behandeld.

P. Veltman

Compact (R) is een uitgave van

KPMG Klynveld EDP Audit

Deze informatie is in de eerste plaats bestemd voor degenen die in de algemene controlepraktijk werkzaam zijn van KPMG Klynveld Kraayenhof & Co. De in dit tijdschrift weergegeven meningen mogen niet altijd gezien worden als officiële zienswijze van KPMG Klynveld EDP Audit. De in rubrieken besproken tijdschriften, boeken en artikelen worden soms geheel opgenomen of verkort aangehaald, tevens als regel voorzien van commentaar.

Redactie:
A.W. Neisingh
D. Steeman
P. Veltman
H.J.M. van der Wielen

Adres:
World Trade Center Amsterdam
Strawinskylaan 1257
Toren D 11e etage
1077 XX Amsterdam
Telefoonnummer: 020 - 5461911

Postadres:
Postbus 72001
1007 TB Amsterdam

ISSN 0920-1645

Indien u belangstelling heeft voor meerdere exemplaren kunt u deze aanvragen op bovenstaand adres, evenwel zolang de voorraad strekt.

DE GEVOLGEN VAN TOEPASSING VAN INFORMATIETECHNOLOGIE VOOR BANKEN[1]

door ir. S.L. Lelieveldt

1 Inleiding

Ontwikkelingen in de informatietechnologie hebben veel en grote gevolgen voor ondernemingen en consumenten. Een goed voorbeeld hiervan is de streepjescode (uniforme artikelcodering). Deze wordt gebruikt bij het transport van produkten van de fabriek naar de groothandel, bij de verspreiding van die produkten naar de detailhandel en ten slotte bij het afrekenen van de produkten aan de kassa. De voordelen hiervan zijn onder andere een snellere afhandeling bij de kassa, het verbeteren van het voorraadbeheer, betere marktonderzoeken en eenvoudiger bestelprocedures.

Een ander voorbeeld wordt gegeven door McFarlan.[2] Hij beschrijft hoe een distributeur bij alle grote klanten een order-entry-systeem plaatst, zodat deze klanten hun orders direct in het computersysteem van de distributeur kunnen invoeren. De klant kan zo sneller en beter orders doorgeven en de distributeur hoeft de orders niet nogmaals in te voeren, waardoor de kans op fouten wordt verkleind.

Naast directe voordelen voor beide partijen heeft het invoeren van dit systeem ook tot gevolg gehad dat de verkopen van de distributeur toenamen ten koste van een belangrijke concurrent. De concurrent werd hierdoor zelfs genoodzaakt om grote reorganisaties door te voeren, maar deze waren slechts ten dele succesvol. De gevolgen van een doordachte toepassing van technologische ontwikkelingen blijven dus niet alleen beperkt tot efficiëntievoordelen, maar leiden ook tot een voorsprong op de concurrentie.

Een interessante vraag is nu hoe de banken (kunnen) omgaan met de ontwikkelingen en toepassingen van de informatietechnologie. Een groot deel van de maatschappelijke geldhoeveelheid bestaat immers uit een aantal bits in de bankcomputer. Banken zijn hierdoor bij uitstek in staat om met gebruikmaking van de informatietechnologie concurrentievoordelen te behalen.

In dit artikel zal ik bovenstaande vraag proberen te beantwoorden aan de hand van het bedrijfstakmodel van Porter. Voordat ik echter aangeef welke gevolgen de ontwikkelingen van de informatietechnologie in de toekomst kunnen hebben, zal ik ruim aandacht besteden aan de kenmerken van de concurrentie in de banksector. Daarom wordt in paragraaf 2 het model van Porter geïntroduceerd en toegelicht aan de hand van de geschiedenis van de banksector.

Vervolgens wordt in paragraaf 3 stilgestaan bij het ontstaan van het elektronisch betalen in Nederland. Het zal blijken dat het gedrag van de verschillende banken voor een belangrijk deel te verklaren is uit overwegingen met betrekking tot de onderlinge concurrentie en in mindere mate door overwegingen met betrekking tot de mogelijkheden van de informatietechnologie. Hoewel alleszins begrijpelijk, is een dergelijke reactieve houding met het oog op de toekomst niet gewenst.

In paragraaf 4 wordt dan ook aangegeven wat die toekomstige ontwikkelingen zijn en welke gevolgen ze kunnen hebben voor de banksector. Kort samengevat komt het erop neer dat de banksector rekening moet houden met een grotere concurrentie en het overbodig worden van bepaalde financiële diensten, tenzij men erin slaagt hieraan een eigen meerwaarde toe te voegen.

---

1 Dit artikel (ingezonden juli 1989) is een bewerking van het verslag *Informatietechnologie in de banksector* dat door de auteur in 1988 in het kader van het vak impact van de automatisering is geschreven.

2 McFarlan, F.W., Information technology changes the way you compete, *Harvard Business Review*, mei-juni 1984, jrg 62, nr 3, pp 98-103.

2 Het model van Porter beschreven en toegelicht

Het bedrijfstakmodel van Porter is in de zeventiger jaren aan de Harvard Business School ontstaan als een hulpmiddel bij de analyse en ontwikkeling van ondernemingsstrategieën. Hoewel relatief jong (1980) is het nu al klassiek te noemen.[1]

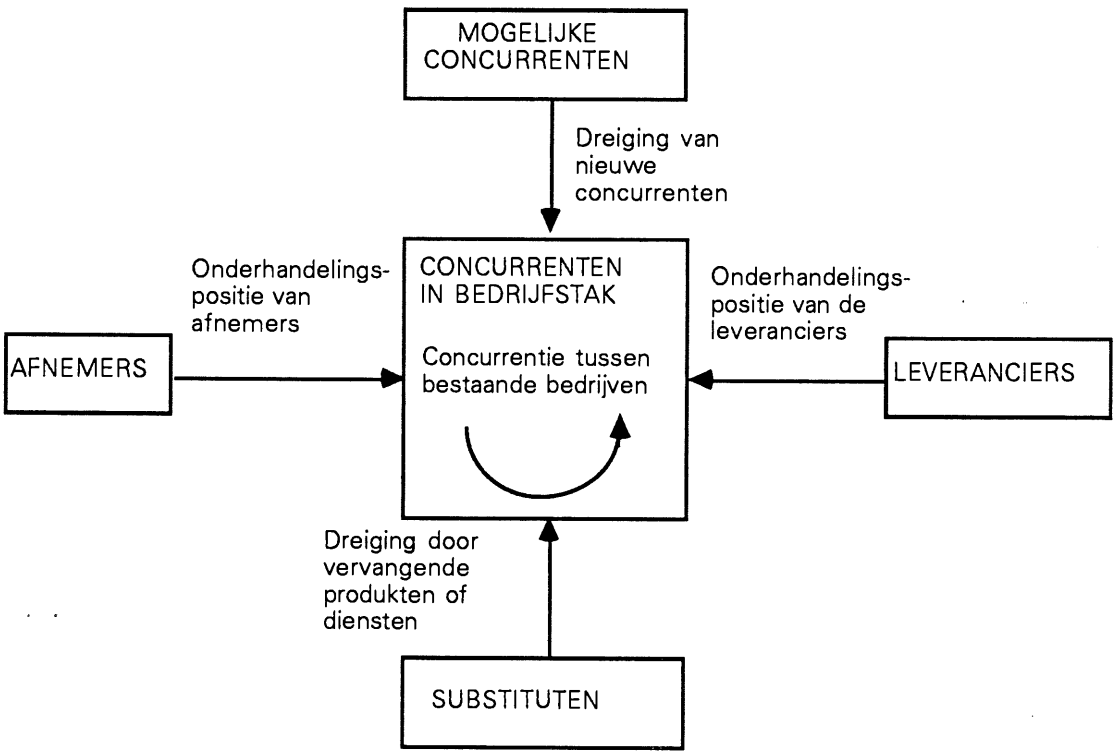
In dit artikel pas ik het model toe op de banksector. Een bank beschouw ik hierbij als: "een instelling welker bedrijf bestaat in het verlenen van kredieten, welke zij verschaft, hetzij uit eigen of van derden opgenomen middelen, hetzij door de creatie van nieuw ruilmiddel."[2]

Het primaire proces van een bank bestaat uit het opnemen en/of het uitlenen van geld in verschillende vormen en uit alle activiteiten die daarmee verband houden. Het opnemen van gelden wordt het passieve bankbedrijf genoemd. Het uitlenen van gelden is het actieve bankbedrijf.

Banken verrichten verder een aantal functies die met het actieve en passieve bankbedrijf samenhangen. Het betreft hier bijvoorbeeld de handel in vreemde valuta, effecten en assurantiebezorging of het optreden als executeur-testamentair, reisbureau en belastingconsulent.

Het model van Porter is weergegeven in onderstaande figuur en maakt een onderscheid in vijf factoren, die de positie van een onderneming in de bedrijfstak bepalen, te weten de positie van afnemers en leveranciers, de dreiging door substituten of nieuwe concurrenten en de concurrentie tussen bestaande ondernemingen.

Figuur 1: Concurrentiefactoren in een bedrijfstak
Bron: Porter, 1980, p 4.



1 M.E. Porter, *Competitive strategy*, New York, 1980. Zie voor verdere uitwerking van de stof ook:M.E. Porter, *Competitive advantage*, New York, 1984.

2 F. de Roos en D.C. Renooij, *De algemene banken in Nederland*, Leiden, 1976, p 6.

Als toelichting op het model zal ik aan de hand van de concurrentiefactoren een beschrijving geven van de ontwikkelingen in de banksector.

Afnemers
Voor de tweede wereldoorlog was er sprake van een grote hoeveelheid banken, die zich elk op een eigen terrein begaven en die elk verbonden waren met een eigen groep afnemers.[1]

Zo verleenden de algemene banken kredieten op korte termijn aan het bedrijfsleven en effectencliënten, bemiddeling bij de handel in effecten, verzorgden zij de emissie van aandelen en obligaties en ontvingen zij termijndeposito's. Het betalingsverkeer verzorgden zij vooral ten behoeve van ondernemingen onderling en de overheid. Het betrof veelal grote bedragen. Spaargelden namen zij zo goed als niet aan.

De girodiensten (Postcheque- en Girodienst) legden zich toe op de afwikkeling van het betalingsverkeer met name ten aanzien van kleinere bedragen tussen ondernemingen, particulieren en overheid. De spaarbanken en de Rijkspostspaarbank boden de gelegenheid om op veilige wijze geld te sparen. Hierbij trokken zij vooral spaarders uit grote en kleine steden aan.

De coöperatieve banken verleenden kort en middellang krediet aan boeren, tuinders, coöperaties en middenstanders in de plaatselijke gemeenschap en verzorgden een relatief klein deel van het binnenlandse betalingsverkeer. Effecten- en deviezenzaken en het emissiebedrijf kwamen slechts bij uitzondering voor. Van overwegend belang was het aantrekken van spaargelden van spaarders uit het platteland.

Het einde van de oorlog bracht echter een aantal belangrijke veranderingen met zich mee. Ten eerste werd de consument zich - dankzij de geldzuivering van 1945 - bewust van het bestaan van bank- en giro-instellingen. Ten tweede was er in verband met de wederopbouw gaandeweg meer behoefte aan geld in de particuliere sector.

Gezien het feit dat de traditionele financieringsbronnen (deposito's van welgestelden en ondernemingen) ontoereikend waren en dat inflatoire financiering van de overheid (het bijdrukken van geld) niet wenselijk werd geacht, waren de algemene banken vanaf de jaren zestig aangewezen op nieuwe financieringsbronnen.

Leveranciers
De nieuwe financieringsbronnen werden gevonden in het aantrekken van spaargelden van particulieren. De particuliere rekeninghouder was dus voor de algemene banken vooral interessant als leverancier van geld. Dit kon vervolgens worden uitgeleend aan het bedrijfsleven ten behoeve van het herstel van de economie.

De rust in de banksector werd hierdoor verstoord en de banken begonnen zich meer en meer op elkaars - voorheen zo mooi afgebakende - terrein te begeven. Niet alleen werd geprobeerd om elkaars klanten te binden, maar ook werd de dienstverlening uitgebreid. Omdat het traditionele verschil tussen bankinstellingen vervaagde, werd dit verschijnsel branche-vervaging genoemd.

Het kiezen voor de particuliere rekeninghouder als leverancier had vooral gevolgen voor de Postgiro. Deze had in 1960 met 825.000 rekeninghouders vrijwel 100% van de markt in handen. De positie van de Postgiro werd dus bedreigd.[2]

Substitutie
Tegen het eind van de jaren vijftig deed zich door de optredende administratieve automatisering de mogelijkheid voor om loon- en salarisbetalingen op girale wijze te verrichten. Met name

---

1 Afkomstig uit: H.W.J. Bosman, *Het Nederlandse bankwezen*, Deventer, 1983.

2 Zie voor gedetailleerdere beschrijving: M. Peekel en J.W. Veluwkamp, *Het girale betalingsverkeer in Nederland*, Deventer, 1984, dat een belangrijke basis vormde voor dit artikel.

werkgevers en overheid zagen hierin een goede mogelijkheid om op de dure, arbeidsintensieve procedure van contante uitbetaling te bezuinigen.

De Postgiro speelde met de al langer bestaande postrekening als eerste op deze behoefte in. Lonen en salarissen werden in toenemende mate op deze rekeningen gestort. Er vond - in termen van Porter - substitutie plaats van menselijke arbeid en van chartaal geld. Beide werden vervangen door respectievelijk een machine-gebaseerde procedure en toezending van een afschrift.

De banken constateerden gaandeweg dat veel van de aan het bedrijfsleven verstrekte fondsen door de loonbetalingen uit het bankcircuit verdwenen naar de Postgiro-rekeningen. Dit beperkte hun kredietruimte terwijl de vraag naar kredieten bleef toenemen. Om deze ontwikkeling te bestrijden volgden de banken snel in het spoor van de Postgiro en boden zij aan zo veel mogelijk inkomenstrekkers girale overboekingsfaciliteiten aan.

Dit was echter niet genoeg. Ondanks het feit dat steeds meer loonbetalingen giraal werden verricht, bleken de rekeninghouders direct nadat dit geld bijgeschreven was naar de bank te gaan om het geld op te nemen. Voor de algemene banken betekende dit een grote en ongewenste toename van onrendabele transacties.

In 1967 werden daarom drie instrumenten ingezet om de girale tegoeden binnen het bankcircuit te houden; de BankGiroCentrale (BGC), de rentegevende salarisrekening en de betaalcheque. Hierdoor werden loonzakje en bankbiljetten gesubstitueerd door de (voor banken goedkopere) salarisrekening en gegarandeerde cheque.

Met de oprichting van de BGC zetten de algemene banken, de coöperatieve banken en de Spaarbanken een geïntegreerd, geautomatiseerd bankgirocircuit op. De traditioneel beperkte verwerkingscapaciteit van dit circuit werd zo opgeheven en hierdoor waren de banken in staat om in hoog tempo grote hoeveelheden betalingsopdrachten te verwerken. Ook konden zij hierdoor - in navolging van de Postgiro - faciliteiten als automatische salarisbetaling, incasso en periodieke overboeking aanbieden.

Een tweede instrument waarmee de banken de concurrentieslag om de particuliere rekeninghouder met de Postgiro aangingen was de rentegevende salarisrekening. Net als bij de Postgiro was het gebruik van deze rekening gratis. De banken vergoedden bovendien een rente van 3,5%, terwijl op grond van wettelijke bepalingen de postrekening niet rentegevend was.

De betaalcheque werd op initiatief van de door een aantal grote banken opgerichte Stichting Bevordering Chequeverkeer ontwikkeld.[1] Doordat de banken de uitbetaling van de cheque (aanvankelijk tot een maximum van 50 gulden) garandeerden, raakte de betaalcheque al snel ingeburgerd.

De oprichting van de BGC en de introductie van de betaalcheque betekenden een aantasting van de sterke positie van de Postgiro. Zij introduceerde daarom de girobetaalkaart en een aan de postrekening gekoppelde renterekening van de Rijkspostspaarbank. Hierop werd ook 3,5% rente vergoed, maar in de praktijk bleek het publiek deze als minder aantrekkelijk te ervaren.

Concurrentie

Uit het voorgaande blijkt dat de concurrentie in de bankwereld aanvankelijk zeer beperkt was. Toen er behoefte was aan meer krediet voor het groeiende en uitdijende bedrijfsleven kwam de particuliere rekeninghouder in zicht. Zodoende nam de concurrentie toe, hetgeen in het voordeel was van de consument.

1 Het concept van de gegarandeerde betaalcheque was al in 1959 door de Twentsche Bank geïntroduceerd, maar bleek in de markt niet levensvatbaar. Ook had De Nederlandsche Bank juridische bezwaren tegen het betaalmiddel, waardoor het experiment reeds in 1962 werd beëindigd (R.E. de Rooy, *De betaalcheque*, Deventer, 1985, p 4).

Een ander gevolg van de toenemende behoefte aan kredieten voor het bedrijfsleven bestond uit het samengaan van banken. Dit verschijnsel wordt concentratie genoemd. Het bood de banken de mogelijkheid om te profiteren van een meer efficiënte bedrijfsvoering en had als voordeel dat de banken meegroeiden met de ondernemingen aan welke ze krediet verstrekten.[1]

De banksector veranderde door de concentratie en de branche-vervaging. Van een markt met veel verschillende aanbieders met elk een eigen afnemersgroep werd het een markt met weinig aanbieders, die concurreerden om dezelfde afnemers. Na afloop van het gevecht om de particuliere rekeninghouder waren de verhoudingen ingrijpend veranderd ten nadele van de girodiensten.

Waar de girodiensten in 1960 vrijwel 100% van de particuliere betaalrekeningen beheerden was dit percentage in 1970 gedaald tot 48%. De resterende 52% was verdeeld onder de algemene banken (21%) de coöperatieve banken (25%) en de spaarbanken (6%).

Een belangrijke vraag is of de banksector in het begin van de jaren zeventig beschouwd kan worden als een markt met volledige concurrentie. In mijn ogen is dat niet het geval. Hoewel de intensiteit van de concurrentie toenam, verminderde het aantal concurrenten. Deze lieten zich vooralsnog leiden door het streven naar meer particuliere rekeninghouders boven een streven naar beheersing van de kosten.[2]

Hieruit trekt de heer Eizenga de conclusie dat de banksector te kenschetsen is als een oligopolie: "Daarbij krijgen overwegingen met betrekking tot opbrengsten en kosten aanvankelijk minder accent dan het streven de afzet - in dit geval de dienstverlening aan de cliënten - uit te breiden. Wanneer echter een bepaalde vorm van dienstverlening minder rendabel is, zullen de aanbieders ervan dit op den duur ervaren en zullen kosten- en opbrengstoverwegingen meer gewicht krijgen."[3]

Nieuwe concurrenten

Hoewel algemene banken zonder problemen betalingsfaciliteiten aan de particuliere rekeninghouder konden aanbieden, was het voor de Postgiro minder eenvoudig om de zakelijke markt van de algemene banken te betreden. Het assortiment van de Postgiro was in de wet omschreven en kon slechts na politieke toestemming worden uitgebreid.

Het bestaan van een wettelijke of andere belemmering (een gepatenteerd produktieproces bijvoorbeeld) om te kunnen concurreren op een bepaalde markt wordt door Porter entry barrier genoemd. Pas als deze drempel genomen is, is een onderneming een concurrent. Omdat het publiek een voorkeur had voor het bij één bank betrekken van alle financiële diensten, verloor de Postgiro in de jaren zeventig gestaag klanten.

Een laatste ontwikkeling in de jaren zeventig is de opkomst van nieuwe financiële instellingen, zoals de Robeco-groep, die zonder kantorennetwerk goedkoop wisten te opereren. Terzelfder tijd verslechterde de economische situatie, waardoor de consument op zoek ging naar de voordeligste spaarfaciliteiten.

De particuliere rekeninghouders roomden dus massaal hun tegoeden af en brachten deze onder bij dergelijke instellingen. De banken droegen hierdoor wel de lasten (kosten) maar niet de lusten (uitlenen van spaargeld) van de relatie met de particuliere rekeninghouder.

Strategieën

De hierboven aangehaalde concurrentiefactoren verklaren slechts ten dele de verhoudingen in

---

1 Zie ook:F. de Roos en D.C. Renooij, *De algemene banken in Nederland*, Leiden, 1976, p 37.

2 Begin jaren 70 blijken de kosten van het betalingsverkeer hoger dan verwacht (mede veroorzaakt door de uitgebreide kantorennetwerken). Hoewel deze kosten aanleiding zouden kunnen geven tot het invoeren van een bepaalde vorm van tarifering besluiten de banken het te vergoeden rentepercentage te verlagen.

3 W.Eizenga schreef: Banken en het betalingsverkeer van gezinshuishoudingen, 1972, pp 22-23.

een bedrijfstak. Het is minstens even zinvol om een beeld te hebben van de naaste concurrenten. Welk gedrag is van hen te verwachten, kortom welke strategie volgt de concurrent? Porter noemt drie strategieën die een onderneming kan kiezen om beter te presteren dan de concurrentie, te weten kostenvoordeel, differentiatie en focus.[1]

De strategie van het kostenvoordeel kan gebaseerd zijn op het concept van de leercurve. De kosten van het produceren van één produkt zullen dan afnemen naarmate er meer ervaring is opgedaan met het produktieproces. Kostenvoordelen kunnen ook het gevolg zijn van een gunstige locatie ten opzichte van de grondstoffen of van een groot marktaandeel.

De differentiatiestrategie is gebaseerd op het creëren van een unieke positie in de bedrijfstak. Differentiatie kan geschieden met betrekking tot naamsbekendheid, kwaliteit, service, technologie of andere aspecten. Hierdoor zal er sprake zijn van een sterke binding van de klant met de onderneming.

De focusstrategie ten slotte bestaat uit het concentreren van de activiteiten op een bepaalde afnemersgroep, produktlijn of geografisch gebied. De strategie berust op de veronderstelling dat de onderneming op die manier de markt beter kan bedienen dan de concurrent. Deze strategie is te combineren met die van het kostenvoordeel of differentiatie.

Bestuderen we de banksector in Nederland[2], dan kunnen we concluderen dat de Postbank een strategie van kostenvoordeel nastreeft. Dit is mogelijk door een groot marktaandeel (bijna 50% van alle rekeninghouders in Nederland) en een efficiënt produktie-apparaat.

De Rabobank (verzameling van het merendeel der coöperatieve banken) daarentegen hanteert een differentiatiestrategie. Zij zal de particuliere rekeninghouder op elke leeftijd de gepaste faciliteiten aanbieden en onderscheidt zich hierbij (of: wenst zich te onderscheiden) van andere banken op het aspect persoonlijke dienstverlening en service.

De algemene banken ABN en Amro hanteren een soortgelijke strategie maar richten zich daarnaast voornamelijk op de grote handels- en industriële bedrijven. De NMB (Nederlandsche Middenstandsbank) daarentegen bedient meer het segment van de kleinere bedrijven en combineert dit met een vernieuwend karakter; wie wat nieuws wil (van chipkaarten tot schuldenruil met derde wereldlanden) is bij de NMB op de juiste plaats.

Een typisch voorbeeld van de focusstrategie is de Friesland Bank. Zij concentreert zich op alle klanten in een bepaalde regio. Een ander voorbeeld is van Lanschot-bankiers, die zich voornamelijk concentreert op rekeninghouders met een goed inkomen.

In de volgende paragraaf zal ik een beschrijving geven van de introductie van het elektronisch betalen in Nederland. Daarna wordt aan de hand van het hierboven beschreven model van Porter een oordeel gevormd over het strategische gedrag van de betrokken ondernemingen in de bedrijfstak.

3 Introductie van het elektronisch betalen in Nederland

Voor deze paragraaf heb ik gebruik gemaakt van een grote hoeveelheid artikelen. Naar de belangrijkste hiervan wordt door middel van noten verwezen.

Het begin van elektronisch betalen met magneetkaart
Het inititatief voor de introductie van een elektronisch betaalnetwerk was afkomstig van de benzinemaatschappijen, die - uit een oogpunt van veiligheid - de voorkeur gaven aan elektronisch in plaats van contant betalen. Aanvankelijk waren de banken niet bereid om hieraan gehoor te

1 M.E. Porter, *Competitive strategy*, New York, 1980, pp 34-46.

2 W. Fiet, Marktpositie van banken is historisch verklaarbaar, *Bank- en effectenbedrijf*, juni 1986, jrg 35, nr 6, pp 186-191.

geven. Toen de benzinemaatschappijen dreigden dan maar met private label-card-organisaties in zee te gaan, besloten de banken om toch aan de oproep gehoor te geven.

Er werd besloten om een 18 maanden durende proef met elektronisch betalen op te zetten in de regio Eindhoven/Tilburg. In 1981 was een eerste functioneel ontwerp van een betaalautomaat gereed. Dit was echter voor de Postbank[1] onaanvaardbaar. Alle betalingen zouden volgens het ontwerp door één computer verwerkt worden, hetgeen technisch onacceptabel was. De verwerking van betalingen verloopt bij de Postbank anders dan bij de andere banken en op dit gebied wenste de Postbank geen concessies te doen.

Later erkende de Postbank dat haar harde opstelling ook ingegeven werd door commerciële overwegingen. Het elektronisch betalen was namelijk één van de weinige diensten waarmee de Postbank zich goed kon profileren in de markt voor de particuliere rekeninghouder. Er werd een tweede functioneel ontwerp gemaakt.

Bij het tweede ontwerp bleek dat het technisch niet eenvoudig was om met één terminal twee verschillende verwerkingsprocessen te ondersteunen. Bovendien bleek de aan- en afmeldingsprocedure van de betaalautomaten nog voor behoorlijke problemen te zorgen. De proef liep derhalve nog meer vertraging op. In plaats van in 1984 werden in november 1985 de eerste betaalautomaten bij pompstations in de regio Eindhoven/Tilburg geplaatst.

Het resultaat van deze proef werd positief genoemd. Uiteindelijk werd 10% van de transacties die voor de proef met name door middel van cheques werden afgehandeld, elektronisch betaald. De gebruikte apparatuur en programmatuur was echter zo ingewikkeld, dat het in stand houden of het uitbreiden van het systeem technisch gezien niet verstandig zou zijn.[2]

Initiatieven met gebruikmaking van een chipkaart
In oktober 1985 hadden Ahold en de NMB een concept-beschrijving van een proef met chipkaarten bij de winkels van Albert Heijn gereed. Voor Ahold waren met name de volgende factoren van belang:
- door elektronisch betalen wordt het betaalproces versneld, hetgeen leidt tot een verhoging van de efficiency;
- het risico en de kosten van het storten van grote bedragen kasgeld worden verkleind;
- het koppelen van elektronisch betalen met automatisch voorraadbeheer en scanning van de produkten (streepjescode) kon onderzocht worden.

De NMB had door de proef de gelegenheid om de reactie van de klanten op elektronisch betalen te onderzoeken en te bestuderen welke gevolgen dit had voor de kosten van betalingen en de procedures bij de bank.

Het midden- en kleinbedrijf begon zich te zelfder tijd ook te realiseren dat de nieuwe ontwikkelingen op het gebied van elektronisch betalen veel invloed zouden kunnen uitoefenen op zijn branche en zodoende verleende het Hoofd Bedrijfsschap Detailhandel (HBD) in juli 1985 aan het Economisch Instituut voor het Midden- en kleinbedrijf (EIM) opdracht tot het opzetten van een praktijkproef elektronisch betalen in de detailhandel. De resultaten van zo'n proef zouden waardevol kunnen zijn in geval er over de vormgeving van elektronisch betalen onderhandeld zou moeten worden met de banken.

Beide voorstellen werden voorgelegd aan de Raad voor Betalingsverkeer (RvB) waarin de banken - zonder Postbank - zitting hebben en de commissie apparatieve voorzieningen. Dit leidde ertoe dat de banken in januari 1986 verklaarden dat zij de initiatiefnemers van een eventuele praktijkproef dienden te zijn. De Postbank en het HBD werden vervolgens uitgenodigd voor deelname aan een proef, doch beide partijen sloegen de uitnodiging af.

---

1 Ik zal voor de duidelijkheid de term Postbank ook gebruiken in die gevallen waar eigenlijk sprake is van de postcheque- en girodienst.

2 Zie ook:H. Kamberg, *Plastic cash*, 1987, pp 45-59.

Hierop werd besloten tot formatie van een stuurgroep, die overeenstemming moest bereiken over een gezamenlijke chipkaartproef. In deze stuurgroep hadden en hebben HBD, consumentenbond, banken, het ministerie van Economische Zaken, de Postbank en vakorganisaties zitting. In juni 1987 was de definitiestudie gereed. Op 1 november 1989 is in Woerden gestart met de proef.

De volgende overwegingen spelen onder andere bij de chipkaartproef op de achtergrond mee:
1. de banken zien niet zoveel in de proef omdat zij in eerste instantie de kosten van het magneetstripkaartsysteem willen terugverdienen. Bovendien zijn zij de mening toegedaan dat de betaalautomaat door de detaillist bekostigd moet worden;
2. de wens van de banken is voor de detailhandel onaanvaardbaar. In hun ogen is het onredelijk om het vooruitgeschoven loket van de bank te moeten betalen. Het Nederlands Christelijk Ondernemers Verbond (NCOV) verwacht daarom dat betalen met de chipkaart pas halverwege de jaren negentig mogelijk zal zijn.

De agressieve Postbank
De Postbank bemerkte dat diverse organisaties plannen hadden op het gebied van elektronisch betalen en met het oog op hun marktpositie en marktpotentieel (vijf miljoen rekeninghouders) besloten zij om positief te reageren op de vraag van Shell om deel te nemen aan een betaalsysteem voor Shell.

Shell had speciaal contact met de Postbank opgenomen, omdat de Postbank aangekondigd had om - in verband met de toenemende fraude met betaalcheques - alle giropassen te vervangen door passen met een magneetstrip. Overigens liet Shell hierbij weten dat als de Postbank niet wilde meedoen, het betaalsysteem zonder de Postbank ontwikkeld zou worden. In juni 1986 maakten Shell en de Postbank derhalve bekend dat zij overeenstemming hadden bereikt over het gebruik van de giromaatpas bij de pompstations van Shell.

De andere banken reageerden verbaasd en enigszins geagiteerd, omdat de proef in de Eindhoven/Tilburg-regio nog steeds liep. De Postbank wees de banken echter op het feit dat de proef elektronisch betalen in principe al afgesloten had moeten zijn. Van een schending van afspraken om tot het eind van de proef geen verdere initiatieven te ontwikkelen was dan ook geen sprake.

De banken moesten daarna wel overleggen met de Postbank over één nationaal betaalsysteem. Indien er ooit zo'n systeem zou komen, was medewerking van de Postbank, gezien haar afspraak met Shell, onontbeerlijk.

Terwijl deze besprekingen in juni 1987 gaande waren maakte de Postbank bekend met Albert Heijn een afspraak gemaakt te hebben voor een proefneming met elektronisch betalen. Wederom waren de banken geïrriteerd, maar de onderhandelingspositie van de Postbank was nu zo sterk, dat de banken de besprekingen over één betaalsysteem niet wilden stopzetten. De kans was groot dat de Postbank anders een onaantastbare voorsprong op het gebied van elektronisch betalen zou krijgen.

De doorbraak
Op 9 december 1987 vierde de BankGiroCentrale haar twintigjarig bestaan. Albert Heijn ging in zijn toespraak aan de verzamelde bankwereld in op de traagheid waarmee de banken tot beslissingen kwamen met betrekking tot het elektronisch betalen. De kern van zijn betoog luidde dat de banken de strategische gevolgen ervan (veranderde concurrentieverhoudingen en eventuele tarifering van betaaldiensten) niet openlijk wensten te bespreken.

Albert Heijn verwoordde dit als volgt:
"Zolang de beleidsmakers van de banken niet tot een echte overeenstemming komen en het elektronisch betalen aan de technici overlaten, mag het ook geen verbazing wekken dat er in de praktijk weinig vooruitgang wordt geboekt. Men mag van technici veel verwachten vandaag de

dag, maar niet dat zij de problemen oplossen waar de beleidsmakers aan de top al jaren met een grote boog omheen lopen."[1]

Deze donderspeech had effect. Nog voor de jaarwisseling kwam officieel de afspraak tussen alle banken tot stand om een infrastructuur te ontwikkelen ten behoeve van het met één bankpas betalen bij betaalautomaten. De afspraak luidde dat de infrastuctuur per januari 1989 gerealiseerd moest zijn.

In november 1988 werden de eerste boodschappen van de minister van Financiën afgerekend met behulp van een betaalpas van de Postbank door Albert Heijn. Hiermee was de eerste niet-experimentele betaalautomaat in werking gesteld. De banken maakten terzelfder tijd bekend het beheer van het betaalnetwerk te hebben ondergebracht in een aparte vennootschap: BeaNet BV.

De oprichting van BeaNet BV verliep overigens niet zonder de nodige opschudding.[2] Zo beschuldigden consumentenorganisaties, detailhandelsorganisaties en computerservicebureaus de banken ervan om het elektronisch betalingsverkeer te willen monopoliseren. Onder druk hiervan besloten de banken tot structureel overleg met onder andere de NCOV en de KNOV over de rechten en plichten van de deelnemers aan het elektronisch betalingsverkeer.

Verder heeft BeaNet BV al het eerste kort geding achter de rug. Het Arnhemse computerbedrijf CCV wenste - als niet aan banken verbonden organisatie - in het bezit te komen van de specificaties van de betaalterminals, zoals die door BeaNet worden voorgeschreven. Het bedrijf slaagde hier niet in en verloor het kort geding. De specificaties werden overigens vanaf 27 januari 1989 door BeaNet BV vrijgegeven.[3]

Beoordeling

De stuwende ondernemingen achter de introductie van het elektronisch betalen in Nederland zijn achtereenvolgens Shell, Albert Heijn en de Postbank. Elk van deze ondernemingen heeft goede redenen gehad om over te gaan tot het elektronisch betalen.

Zo bood dit Shell de mogelijkheid om de veiligheid bij de benzinestations te vergroten en zou Albert Heijn in staat zijn om een aanzienlijk efficiëntievoordeel bij de kassa-afhandeling te bereiken. De Postbank ten slotte kon, vooruitlopend op een toekomstig nationaal betalingscircuit, de rekeninghouders aan zich binden met een makkelijk en veilig betaalmiddel.

De in eerste instantie afwachtende houding van banken ten opzichte van het elektronisch betalen werd door grote afnemers van financiële diensten doorbroken met een dreigement om anders gebruik te maken van substituten (een plastic betaalkaart hoeft niet per definitie door een bank gemaakt te worden). Gezien de concurrentieverhoudingen is het begrijpelijk dat deze partijen met de Postbank overeenstemming konden bereiken.

Dat de banken in Nederland een afwachtende houding hebben aangenomen blijkt uit het feit dat soortgelijke ontwikkelingen in andere landen veel verder zijn. Vaak wordt hiertegen aangevoerd: "Aangezien Nederland, in vergelijking tot andere landen, over een efficiënt betalingssysteem beschikt, is het elektronisch betalen nog een relatief nieuw fenomeen in Nederland."[4]

Hoewel het eerste deel van de bewering waar is, mag het tweede deel daar niet uit afgeleid worden. Dit blijkt bijvoorbeeld uit het feit dat men in (het met Nederland goed vergelijkbare[5]) België al veel eerder is overgegaan tot de introductie van elektronische betalingssystemen[6].

---

1 A. Heijn, speech van 9 december 1987 tijdens lustrumcongres van BankGiroCentrale.

2 *Banken richten bedrijf op voor elektronisch betalen*, NRC Handelsblad, 20-12-1988, p 16.

3 *Bekendmaking BeaNet BV*, De Volkskrant, 27-1-1989, p 10.

4 Het elektronisch betalingsverkeer in Nederland, brief en notitie van de minister van Financiën, 1988-1989, KS 20917, nr 2, p 3.

5 G.R. de Wit, Technologische ontwikkelingen in het Nederlandse bankwezen, *Tijdschrift voor politieke economie*, maart 1987, jrg 10, nr 3, p 44.

6 F. de Ly, p 15, In: *Verslag van de vergadering van de vereniging 'Handelsrecht' 13 november 1987 over juridische aspecten van moderne betaalmiddelen*, Zwolle, 1988.

De afwachtende houding van banken steekt schril af tegen de voortvarendheid waarmee de technische problemen rond het elektronisch betalen zijn opgelost. Terwijl al vanaf 1975 wordt gesproken over de mogelijke toepassing van computers voor verschillende vormen van elektronisch betalen, heeft het tot november 1988 geduurd voordat de consument hiervan profijt had.

Het tijdstip, de tijdsduur en het verloop van de ontwikkeling van het elektronisch betalen in Nederland leiden daarom tot de conclusie dat deze ontwikkeling vooral gedreven wordt door factoren als concurrentie- en kostendruk.[1] Met andere woorden: de markt kenmerkt zich als demand pull. Er wordt meer gereageerd dan vooruitgelopen op ontwikkelingen die voor de banksector relevant zijn.

De banken doen er met het oog op toekomstige ontwikkelingen verstandig aan om deze reactieve houding te veranderen. Ik zal dit in de volgende paragraaf verder toelichten aan de hand van het model van Porter.

4 Toekomstige ontwikkelingen in de banksector

Afnemers
Afnemers van financiële diensten zijn ondernemingen en particuliere rekeninghouders. Voor wat betreft ondernemingen is het niet denkbeeldig dat verdere schaalvergroting door fusies en overnames zal plaatsvinden. De financiële sector kan hierbij behulpzaam zijn en zal daarnaast zelf ook een of andere vorm van schaalvergroting of concentratie moeten ondergaan.

Een belangrijk punt is de afhankelijkheid van de bank. Door gebruikmaking van een technisch complex en moeilijk vervangbaar systeem, kan de situatie ontstaan dat de onderneming te strak met de bank is verbonden. Als het wisselen van bank de onderneming veel geld kost, kan de bank haar onderhandelingspositie door geleidelijke stijging van tarieven uitbuiten. Ondernemingen moeten daarom op hun hoede zijn bij het accepteren van op het oog voordelige aanbiedingen van banken. Hoe makkelijk is de weg terug?

De consumenten zullen in toenemende mate veeleisend en mobiel worden. Door een klantgerichte instelling en specifiek toegesneden diensten kan de bank de relatie met de rekeninghouder strakker aantrekken. Dit is van belang omdat de particuliere rekeninghouder niet alleen afnemer maar ook leverancier van de bank is.

Leveranciers
Zoals al aangegeven is de relatie van de bank met haar particuliere rekeninghouder erg belangrijk. Pollock merkt hierover op dat:
"All strategies of financial firms must contend with the fact that most financial services are a nuisance from the point of view of the customer."[2]

Vervolgens construeert hij een strategiematrix met als dimensies de aard van het distributiesysteem (persoonlijk/onpersoonlijk) en de aard van de dienst (standaard/op maat). Daaruit blijkt dat een overgang van een chequesysteem naar een elektronisch betaalsysteem niet alleen technisch, maar ook strategisch van aard is.

Het op de oude voet doorgaan met het verlenen van traditionele bankdiensten ziet hij verder als een strategie die in een goed concurrerende markt niet levensvatbaar is. Banken die nu in een beschermde markt opereren moeten zich hiervan bewust zijn en hun toekomstige strategie goed kiezen.

Substituten
De dienstverlening van banken leent zich goed voor substitutie omdat er sprake is van girale

1 Zie ook:W. de Boer, *De behoeften van gebruikers; rol van de overheid.* p 10, (In: WTC Electronics, *Electronisch bankieren*, Utrecht, 1987).

2 Pollock, A.J. , Banking: time to unbundle the services ?, *Long range planning*, januari 1985, jrg 18, nr 1, p 38.

tegoeden. Dienstverlening bij andere instellingen waarin men vertrouwen heeft voldoet immers net zo goed, zolang er de garantie is dat eventuele vorderingen binnen een bepaalde termijn liquideerbaar zijn. Read drukt dit als volgt uit:
"There does seem to be considerable scope for a reduction in the intermediation of banks and its being technology-driven."[1]
Een soortgelijke dreiging is momenteel aanwezig op de consumentenmarkt voor plastic geld door de potentiële uitwisselbaarheid van private-label-pasjes, bankpasjes en creditcards.

Concurrentie
In dit artikel is geconcludeerd dat de concurrentie in Nederland vooralsnog te kenmerken is als oligopolistisch; weinig aanbieders, die elkaar goed in de gaten houden en zich bij elke actie afvragen welke reactie dit tot gevolg kan hebben. In dit licht is het interessant om te onderzoeken welke gevolgen "1992" zal hebben op de banken die zich verzameld hebben in de European Council for Payment Systems (ECPS).

In de ECPS heeft zich een aantal banken verenigd, die afspraken hebben gemaakt met betrekking tot wederzijds gebruik van gelduitgifte-automaten. Zodoende zal een Europees netwerk werkelijkheid kunnen worden. De vraag is nu of en hoe concurrenten uit het creditcard-segment hierop zullen reageren.

Nieuwe concurrenten
Volgens Read brengen de hoge kosten van een grote schaal van financiële dienstverlening met zich mee dat de barrières voor nieuwe concurrenten groter zullen worden.[2] Bestaande concurrenten zouden het de banken echter behoorlijk moeilijk kunnen maken. Zeker als de banken volharden in hun reactieve demand-pull-houding, is de kans niet denkbeeldig dat zij door meer klantgerichte concurrenten worden afgetroefd.

De beste marktpositie lijkt weggelegd voor de bank die er op een effectieve wijze in slaagt om haar toeleveranciers en afnemers van geld aan zich te binden door het aanbieden van of door het delen in financieel getinte ondersteunende voorzieningen. Het betreft bijvoorbeeld het aanbieden van een goede infrastructuur voor het realiseren van de door een onderneming gewenste financiële voorzieningen (netwerken en dergelijke), het aanbieden van opleidingen hierover aan het personeel, het bijhouden van relevante financiële innovaties en advisering over het operationele financieel beheer van de onderneming.

Conclusie
Naarmate de toepassingen van informatietechnologie verder doordringen in de economie zullen banken zich hiervan rekenschap moeten geven. Het gewicht van de economische benadering van financiële dienstverlening neemt zodoende af ten opzichte van een technische benadering. Aan de banken nu de uitdaging om op technologisch gebied bij te blijven.

Als de banken hier niet in slagen, lopen zij het risico dat girale tegoeden wegvloeien naar andere organisaties. Dit hoeven niet eens financiële instellingen te zijn. Een hechte bedrijfstak zou goed in staat zijn een fictieve geldeenheid te ontwikkelen en alle handel daarmee te betalen. Waarmee de mens zou terugkeren naar het principe van de ruilhandel.

1 C.N. Read, Information technology in banking, *Long range planning*, april 1983, jrg 16, nr 4, p 27.

2 ibid.

ELECTRONIC DATA INTERCHANGE (EDI) EN ELEKTRONISCH BETALINGSVERKEER

door M. Groesz

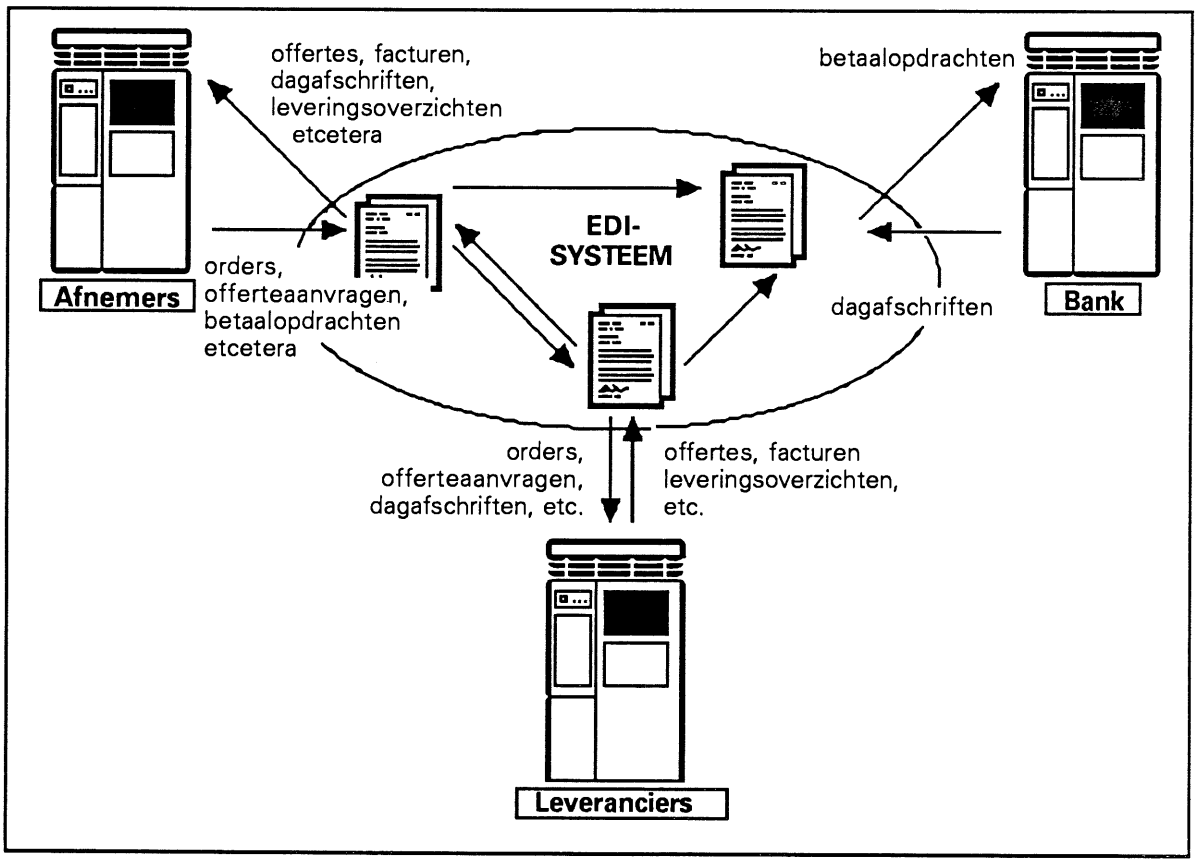
Inleiding

De huidige ontwikkelingen op het gebied van telecommunicatie en informatica, samen telematica genoemd, hebben steeds meer invloed op het communicatieproces tussen handelspartners. Aanwijzingen hiervoor zijn de opkomst van elektronisch betalen en het in toenemende mate elektronisch uitwisselen van gegevens, vaak aangeduid met EDI (Electronic Data Interchange). EDI is de algemeen gebruikte term voor de elektronische verzending van berichten, zoals orders, facturen, transportinstructies en betaalopdrachten tussen ondernemingen met behulp van telecommunicatiefaciliteiten en computers.

In dit artikel zal onder meer worden ingegaan op de betekenis van EDI en wat de drijfveren zijn achter de ontwikkelingen op dit gebied. Vervolgens zal worden ingegaan op de consequenties van EDI voor controlewerkzaamheden en beheersaspecten in het algemeen en op de consequenties voor het betalingsverkeer in het bijzonder.

Ontwikkelingen

In onderstaande figuur wordt het gebruik van EDI geïllustreerd. Aangesloten organisaties communiceren met een EDI-systeem. Het EDI-systeem zorgt voor de juiste aflevering van de diverse berichten.



Illustratie EDI-systeem

De ontwikkelingen op het gebied van EDI worden door sommigen een nieuwe revolutie in de handel genoemd. Voorlopig blijkt het definiëren van een algemeen aanvaarde standaard nog een probleem, dat opgelost moet worden alvorens EDI massaal intrede zal kunnen doen.

Een aantal Nederlandse bedrijven ontplooit reeds activiteiten op het gebied van EDI. In de Rotterdamse haven neemt een aantal bedrijven deel aan het INTIS[1]-project, op de luchthaven Schiphol is het CARGONAUT[2]-systeem reeds enige tijd operationeel en bij de douane is sinds enige tijd het SAGITTA[3]-systeem in werking getreden. Ook in de detailhandel is een EDI-systeem operationeel, TRANSCOM[4] genaamd, waarbij de stichting UAC[5] een belangrijke rol speelt. Het interbancaire systeem S.W.I.F.T.[6] kan eveneens worden geschaard onder de noemer van EDI-systemen.

Daarnaast wordt in toenemende mate door banken de mogelijkheid geboden van het elektronisch bankieren. Hierbij kunnen enerzijds langs elektronische weg betaalopdrachten aan de bank worden aangeboden, anderzijds kan door de bank op verzoek van haar cliënt financiële informatie verstrekt worden.

De ISO[7]-norm voor het elektronisch berichtenverkeer EDIFACT[8], die reeds in 1987 geannonceerd is, heeft voor de meeste van deze systemen als uitgangspunt gediend. In deze norm wordt een beschrijving gegeven van de opbouw van een willekeurig bericht. Meer gedetailleerde beschrijvingen van specifieke berichten worden gevat in de UNSM[9]-standaards, waarvan bij het schrijven van dit artikel slechts de standaard voor de factuur gereed was.

Waarom EDI?

Gebruik maken van EDI is zeer aantrekkelijk door de potentiële voordelen die het in zich heeft. Hieronder wordt een aantal mogelijke voordelen nader beschreven.

Lange tijd was de transportsnelheid van de goederenstroom vrij laag. Hierdoor was het geen probleem om begeleidende documenten met de goederenstroom mee te zenden. Met de snelle transporten van tegenwoordig leidt de afhandeling van begeleidende documenten tot relatief grote vertragingen. Indien gebruik wordt gemaakt van elektronische documenten, dan ontstaat de mogelijkheid documenten voor de goederen uit te zenden. Met name bij grensoverschrijdende transporten kan dit tot tijdsbesparingen van betekenis leiden.

Het voordeel van mogelijkheden voor hogere snelheden in de afhandeling van orders, leidt tot het kunnen garanderen van een snellere aflevering, "just-in-time (JIT) delivery". Het hierdoor kunnen beperken van de voorraad, is een directe besparing ten gevolge van JIT.

De kosten van papieren documenten behorende bij een willekeurige goederenstroom, worden in artikelen die over EDI verschenen zijn gemiddeld geschat op maar liefst 7% van de totale waarde van die goederenstroom. Indien gebruik wordt gemaakt van elektronische documenten, kunnen deze kosten aanzienlijk worden teruggebracht.

---

1 INTIS = Internationaal Transport Informatie Systeem
2 CARGONAUT = Air Cargo Automation
3 SAGITTA = Systeem voor Automatische Gegevensverwerking met betrekking tot Invoeraangiften met Toepassing van Terminals voor het doen van Aangiften
4 TRANSCOM = Transactie Communicatie
5 UAC = Uniforme Artikel Codering
6 S.W.I.F.T. = Society for Worldwide Interbank Financial Telecommunication
7 ISO = International Standards Organization
8 EDIFACT = Electronic Data Interchange For Administration Commerce and Transport
9 UNSM = United Nations Standard Message

De gegevens van een factuur, gewoonlijk afkomstig uit een computersysteem, worden in de meeste gevallen door de ontvanger overgenomen in zijn eigen computersysteem. Het overnemen van deze gegevens is met name bij grote hoeveelheden een inefficiënt proces. Bovendien kunnen bij het overnemen van deze gegevens fouten ontstaan. Weliswaar kunnen deze fouten achteraf worden gecorrigeerd, maar ook dat kost tijd en geld.

Indien door organisaties wordt gecommuniceerd door middel van EDI, dan dwingt dit de organisaties tot standaardisering van het bericht. Het bericht bevat alleen de benodigde informatie in een vaste vorm. Hierdoor is de kans op onduidelijkheden in het bericht ten opzichte van traditionele documenten kleiner.

De uniformiteit van het bericht kan ook bij opslag binnen het eigen computersysteem voordelen bieden. Alle gegevens (ordergegevens, factuurgegevens en dergelijke) zullen in een homogene vorm zijn opgeslagen, hetgeen het uitvoeren van geautomatiseerde controles vereenvoudigt. Het vergelijken van het order- en het factuurbestand, teneinde een controle uit te voeren op het factureren van de binnengekomen en afgehandelde orders, is hiervan een mogelijke toepassing. De strategische gevolgen van EDI kunnen het meest ingrijpend zijn, met name voor de concurrentiepositie. Een "kongsi" van bedrijven in een gezamelijk EDI-systeem kan leiden tot een zogenaamde "prime-vendor"-relatie, waarbij een voorkeur bestaat om met elkaar zaken te doen.

In de praktijk blijkt echter ook vaak het omgekeerde. Door dominante organisaties in een bepaald marktsegment wordt aan leveranciers of afnemers deelname aan haar EDI-systeem opgedrongen, omdat zij anders besluiten voor betreffende ondernemingen een ander te zoeken. In de toekomst zal steeds minder van het verkrijgen van een verbeterde concurrentiepositie ten gevolge van EDI sprake zijn, als wel het verslechteren van de concurrentiepositie als niet aan EDI-projecten wordt deelgenomen terwijl de concurrentie dat wel doet.

Juridische aspecten

In 1987 is door de werkgroep "Moderne Transactie Communicatie" (MTC) van de Commissie van Informatiebeleid van de Raad van de Centrale Ondernemingsorganisaties (CIB/RCO) een tweetal studies verricht naar de fiscale en juridische consequenties van EDI. Dit heeft uiteindelijk geleid tot de oprichting van de stichting EDIFORUM.

De juridische consequenties van EDI houden verband met de omstandigheid dat de wetgeving voornamelijk (nog) gebaseerd is op papieren documenten. Hierdoor komen vragen op omtrent de bewijskracht en de bewaarverplichtingen van een elektronisch bericht en de rechtsgeldigheid van een elektronisch gesloten overeenkomst.

Het feit dat in de huidige wetgeving vooralsnog weinig tot niets is geregeld, dwingt organisaties tot het sluiten van uitgebreide contracten bij een gezamenlijk EDI-project. Dergelijke contracten dienen bepalingen omtrent de beveiliging van het berichtenverkeer, procedures bij het ontvangen van dubbele berichten, verlies of verminking van berichten, aansprakelijkheid, bewijs, arbitrage en bewaring te bevatten.

Consequenties voor de controle

De ontwikkelingen op het gebied van EDI kunnen in het ruimere kader van automatisering in het algemeen worden geplaatst. Een belangrijke doelstelling van automatisering en dus tevens van EDI is het vergroten van de efficiency. Dit wordt bereikt door het elimineren van papier en het inzetten van steeds minder personeel.

Het verdwijnen van papier kan onder meer consequenties hebben voor de primaire vastleggingen. Voor de controle van de jaarrekening is de volledigheid van de primaire vastleggingen van essentieel belang. Er wordt hierbij dan ook gesproken over basiscontroles (basic controls). Indien ten behoeve

van deze controle niet langer beschikt kan worden over papieren documenten, maar voor het vaststellen van de volledigheid moet worden teruggevallen op een bestand op de computer, zal de accountant hoge eisen dienen te stellen aan de automatiseringsorganisatie. Dit probleem kan door organisaties (deels) worden voorkomen door de primaire vastlegging op een andere wijze te doen plaatsvinden. Er kan hierbij gedacht worden aan vastlegging op een niet wisbaar medium met een grote capaciteit. Het NIVRA heeft in maart 1986 studierapport nummer 18 ("Documentvastlegging") gepubliceerd. In dit rapport worden soortgelijke gevaren behandeld die kunnen ontstaan bij het verfilmen of digitaliseren van documenten. Deze problematiek is hiermee nauw verwant.

Gesteld mag worden dat een document dat langs elektronische weg een organisatie binnenkomt zijn weg door de organisatie op dezelfde wijze vervolgt. Dit betekent voor een aantal interne controleprocedures dat zij hierop dienen te worden aangepast. Hierbij kan bijvoorbeeld gedacht worden aan de factuur. In de conventionele situatie wordt deze na ontvangst voorzien van een blokstempel. De noodzakelijke controles worden vervolgens uitgevoerd, hetgeen kenbaar wordt gemaakt door het plaatsen van een paraaf in het blokstempel op de daarvoor bestemde plaats. In een situatie waarbij dezelfde factuur haar weg door de organisatie op elektronische wijze aflegt kan deze procedure niet worden toegepast. Hierdoor dient deze procedure te worden "vertaald" naar een procedure die in de nieuwe situatie wel werkt. In dit geval kan mogelijk worden gedacht aan een systeem van toegangsbeveiliging met daarin adequate functiescheidingen verankerd.

Een ander aspect, dat minder van belang is voor de controle van de jaarrekening, maar waar met name de EDP-auditor mee te maken zal krijgen, betreft de afhankelijkheid van een organisatie van haar automatisering. De automatisering van het administratieve proces maakt de organisatie in hoge mate afhankelijk van die automatisering; tevens neemt het belang van de beschikbaarheid van de gegevens toe. Als gevolg hiervan zal de organisatie hogere eisen dienen te stellen aan maatregelen die de continuïteit van de geautomatiseerde gegevensverwerking waarborgen.

De consequenties voor de accountantscontrole van deze vorm van communicatie tussen handelspartners hebben de volle aandacht. Het NIVRA heeft in 1988 de werkgroep Documentarm Transactieverkeer (Doctrans) in het leven geroepen. Op het moment van het schrijven van dit artikel heeft nog geen rapportage plaatsgevonden. Dit wordt echter op korte termijn verwacht.

Consequenties voor het betalingsverkeer

De communicatie tussen banken en haar cliënten kan zoals vermeld, eveneens worden gezien als een vorm van EDI. Deze vorm van EDI wordt aangeduid met de term "Electronic Banking". Hierbij kan sprake zijn van communicatie van de bank naar de cliënt (bijvoorbeeld elektronische dagafschriften) of andersom (bijvoorbeeld elektronische betaalopdrachten).

In het betalingsverkeer kan de tendens van het verdwijnen van papieren documenten het best worden waargenomen. In eerste instantie is een duidelijke verschuiving opgetreden van het aanleveren van betaalopdrachten met behulp van papierenoverschrijvingsformulieren naar het aanleveren van betaalopdrachten met behulp van een betaaltape of een betaaldiskette. Deze dienen dan vergezeld te gaan van een geleidebiljet. Op dit moment worden mogelijkheden geboden voor het aanleveren van betaalopdrachten door middel van telecommunicatiefaciliteiten. Deze betaalopdrachten worden niet meer vergezeld van een geleidebiljet.

Het ontbreken van een geleidebiljet bij deze nieuwe wijze van betalen is het belangrijkste verschil tussen het verrichten van betalingen met behulp van telecommunicatiefaciliteiten en het aanleveren van betaalopdrachten met behulp van een betaaltape en/of een betaaldiskette. In het artikel "Geautomatiseerd uitgaand geldverkeer en het frauderisico" van drs. H.C. Kocks RA wordt het getekend geleidebiljet nog aangemerkt als een essentieel onderdeel ten behoeve van de beheersbaarheid. De functie van het getekende geleidebiljet in deze situatie is het waarborgen van de authenticiteit van de opdrachtgever en de integriteit van het bestand met betaalopdrachten. Het feit dat bij het aanleveren van betaalopdrachten met behulp van telecommunicatiefaciliteiten geen gebruik wordt gemaakt van een getekend geleidebiljet wil niet zeggen dat ten aanzien van de authenticiteit en de integriteit geen waarborgen kunnen worden verkregen.

De huidige stand van de techniek biedt voldoende mogelijkheden de authenticiteit en de integriteit op andere wijze te waarborgen. Hierbij moet gedacht worden aan het gebruik van unieke beveiligingscalculators of chipcards gecombineerd met PIN-codes. Door de bank wordt het recht op het verrichten van betalingen ontleend aan het bezit van een beveiligingscalculator dan wel chipcard in combinatie met de kennis van de PIN-code. Daarnaast wordt gebruik gemaakt van versleutelingstechnieken. Dit houdt in dat de verzonden betaalopdrachten worden vertaald naar een geheimtaal gedurende het transport. Alleen de bank is in staat de geheimtaal te vertalen naar de oorspronkelijke betaalopdrachten. Deze beide technieken kunnen zowel authenticiteit van de opdrachtgever als de integriteit van het bericht waarborgen, zodat een papieren geleidebiljet niet langer noodzakelijk is.

Dagafschriften in een elektronische vorm zullen het grootste en het belangrijkste deel vormen van de communicatie van banken naar haar cliënten. Voor deze informatiestroom geldt feitelijk hetzelfde als reeds is opgemerkt in de paragraaf waarin de consequenties voor de controle werden behandeld. Nagegaan dient te worden in hoeverre koppelingen gerealiseerd zijn met andere systemen binnen de organisatie, bijvoorbeeld het grootboek. De mate van integratie bepaalt in hoeverre bestaande procedures van interne controles vertaald moeten worden naar nieuwe werkende procedures. Ten behoeve van de controle van de volledigheid zijn de banken bereid om op verzoek (additioneel) papieren dagafschriften te vervaardigen. Daarnaast wordt op dit moment door de banken veelal periodiek (nog) een papieren mutatieoverzicht verzonden, waarop de totalen van de mutaties van een periode staan vermeld.

De controles die momenteel worden uitgevoerd door de procuratiehouder zullen in de toekomst mogelijk worden uitgevoerd door computerprogramma's. In een dergelijke situatie kan het zijn dat een (elektronisch) binnengekomen factuur, nadat een aantal geautomatiseerde controles is uitgevoerd, rechtstreeks leidt tot het genereren én verzenden van een betaalopdracht. In deze situatie dienen vanzelfsprekend zeer hoge eisen te worden gesteld aan de betrouwbaarheid van de geautomatiseerde gegevensverwerking.

Status quo

De ontwikkelingen op het gebied van EDI zijn in volle gang. De projecten die reeds gaande zijn worden waar mogelijk gekoppeld, wijzigingen worden in de systemen aangebracht waar dat gewenst is en het aantal deelnemers aan EDI-projecten neemt snel toe. Het bijblijven in deze materie is daarom een vereiste. Een probleem zal dat niet zijn, want de consequenties van deze ontwikkelingen zijn meer dan interessant.

VERNIEUWING GEAUTOMATISEERDE VERWERKINGSPROCES VAN HET BETALINGSVERKEER BIJ DE POSTBANK

door drs C.P. Aland RA en A.H. Kuijlaars RA, werkzaam bij de IAD Postbank NV

1 Inleiding

De Postbank, voorheen de Postcheque- en Girodienst en de Rijkspostspaarbank, houdt zich van oudsher bezig met financiële dienstverlening voor de particuliere en zakelijke markt.
Centraal daarbij staat het verwerkingsproces van het betalingsverkeer. Via het verwerkingsproces worden jaarlijks meer dan 800 miljoen transacties verwerkt ten bedrage van in totaal ruim ƒ 1.000 miljard. Binnen dit verwerkingsproces worden tevens de betalingen uitgevoerd die voortkomen uit andere dienstverleningsvormen binnen de bank (sparen, hypotheken, consumptief krediet etc.). Deze activiteiten worden uitgevoerd in 4 girokantoren, 7 codeercentra en 5 computercentra en er zijn in totaal meer dan 6.700 medewerkers bij betrokken.
Onder het verwerkingsproces wordt verstaan het geheel van activiteiten gericht op het verwerken van betaaltransacties (voorbewerking, coderen, controleren, boeken, nacontrole en verzending) en de daarmee nauw verbonden functies.
Het verwerkingsproces is het kernbedrijf van de Postbank en zal in de periode 1990 tot 1997 geheel worden vernieuwd. Hierdoor zal beter ingespeeld kunnen worden op toekomstige commerciële eisen en wensen en op de te verwachten ontwikkelingen in het girale betalingsverkeer.

De Postbank is in hoge mate afhankelijk van de kwaliteit, de efficiency en de betrouwbaarheid van het verwerkingsproces van het betalingsverkeer. Dit vloeit niet alleen voort uit de grote betekenis van het betalingsverkeer voor de Postbank maar ook uit de gekozen marktbenadering (het thuisbank-concept), die een snelle en feilloze geautomatiseerde transactieverwerking en informatievoorziening vergt. Het verwerkingsproces is de slagader van de Postbank. De ontwikkeling, bouw en invoering van het nieuwe verwerkingsproces zal zeer zorgvuldig moeten plaatsvinden en mag niet leiden tot vertragingen in de verwerking van transacties.

In dit artikel wordt in hoofdstuk 2 een typering gegeven van het huidige verwerkingsproces alsmede de belangrijkste motieven om tot vervanging over te gaan. Hoofdstuk 3 beschrijft de plannen voor het nieuwe verwerkingsproces en de organisatiestructuur waarin het tot stand zal komen.
In hoofdstuk 4 wordt ingegaan op de (organisatorische) maatregelen die tijdens het ontwikkelingstraject getroffen worden om er zorg voor te dragen dat er ook een vanuit interne controle- en beveiligingsoptiek adequaat nieuw verwerkingsproces ontstaat. Tot slot wordt in hoofdstuk 5 een samenvatting gegeven.
Voor de goede orde wordt nog opgemerkt dat gezien het Postbank-eigen karakter de vernieuwing van het verwerkingsproces in principe los staat van de fusie met de NMB. Een en ander heeft dus uitsluitend betrekking op het verwerkingsproces van het Postbankdeel van de NMB Postbank Groep.

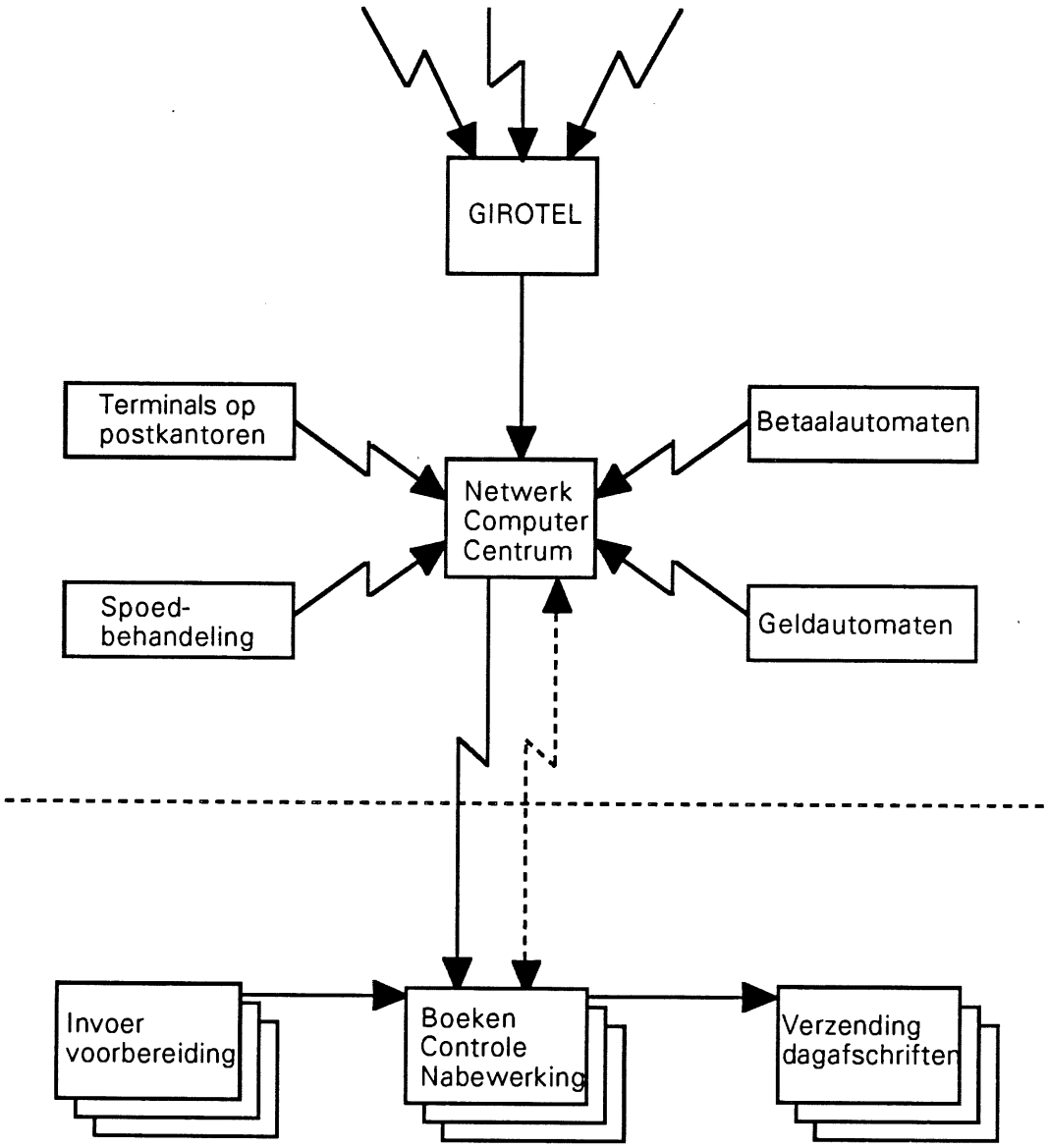
2 Huidige verwerkingsproces

2.1 Typering huidige verwerkingsproces

De opzet van het huidige geautomatiseerde verwerkingsproces is ontwikkeld in het begin van de jaren zestig. Centrale doelstelling was destijds het automatiseren van de toen nog handmatig verrichte boekingshandelingen. Het concept kwam tot stand op basis van de destijds beschikbare technische mogelijkheden, de toenmalige interne organisatie en de toenmalige externe omstandigheden.
Sindsdien is het verwerkingsproces regelmatig aangepast aan de in de tijd veranderende eisen en wensen, bijvoorbeeld:
- de sterke groei van het betalingsverkeer (van 0,8 miljoen girorekeningen in 1960 naar ruim 5,5 miljoen in 1989);

- de koppeling van betaal- en spaarrekeningen;
- de administratief-technische integratie met de Gemeente Giro Amsterdam;
- het geleidelijk opnemen van functies voor het verrichten van maatwerk (voornamelijk voor zakelijke rekeninghouders) in een organisatie die is ingericht voor massale standaardverwerking;
- de ontwikkeling van nieuwe produkten en produktvormen;
- de nieuwe of veranderende eisen (onder andere valutering en snellere doorlooptijd);
- de ontwikkeling van het elektronische betalingsverkeer.

Schematisch en sterk vereenvoudigd is de situatie begin 1990 in figuur 1 weergegeven.
Boven de stippellijn worden de elektronisch betalingsverkeervormen weergegeven. De hieruit voortvloeiende boekingen worden verzameld in het Netwerk Computer Centrum en per dag overgeseind naar de boekingskantoren in Amsterdam, Arnhem en Den Haag.
De elektronische transacties worden te zamen met de hetzij in schriftelijke vorm hetzij in magnetische vorm aangeboden betalingsopdrachten van cliënten batch-gewijs verwerkt.
Per boekingskantoor is hierbij sprake van een eigen girocircuit met een eigen (weliswaar identiek) verwerkingsproces.
De tweezijdige gestippelde datacommunicatieverbinding tussen het Netwerk Computer Centrum en de boekingskantoren staat voor de uitwisseling van saldo-informatie ten behoeve van het geautomatiseerd fiatteren van elektronische betalingsverkeertransacties.



Figuur 1

2.2 Waarom een nieuw verwerkingsproces

Sinds 1960 is het verwerkingsproces aangepast aan veranderende eisen. De nieuwe mogelijkheden van de techniek zijn daarbij in en naast het bestaande systeem ingebouwd.
Omdat systemen destijds niet volledig modulair konden worden opgezet, werken veranderingen/aanpassingen door in een groot deel van het systeem.
Daardoor werd en wordt er veel capaciteit besteed aan het onderhoud van en aanpassingen aan het huidige proces.

In 1987 heeft binnen de Postbank een studie plaatsgevonden naar de toekomstige ontwikkelingen in en rondom het betalingsverkeer, alsmede de gewenste rol van de Postbank als marktleider daarin.
Geconcludeerd werd onder andere dat de flexibiliteit van het verwerkingsproces vergroot dient te worden om in de jaren negentig efficiënt en snel te kunnen inspelen op nieuwe technieken als elektronische betalingsverkeervormen en elektronische documentuitwisseling in combinatie met steeds verdergaande eisen en wensen van cliënten.

Aangezien het huidige systeem nog steeds naar tevredenheid functioneert, en nieuwe functionaliteiten nog steeds kunnen worden ingebouwd, heeft er allereerst een onderzoek plaatsgevonden naar de mogelijkheden van "upgrading" van het bestaande systeem. Uit dit onderzoek bleek dat het bestaande systeem, uiteraard met de nodige inspanningen, tot in het midden van de jaren negentig nog goed zou kunnen functioneren. Daarna zou de druk tot algehele vernieuwing sterk toenemen.

De uiteindelijke conclusie was dat het bestaande verwerkingsproces onvoldoende toekomstvast was en op den duur een keurslijf zou worden met de daarmee gepaard gaande noodzakelijke aanpassingen van de organisatie. Daarom werd besloten de beslissing tot vernieuwing niet uit te stellen. Er werden plannen ontwikkeld voor een modernisering en een andere inrichting van het verwerkingsproces, waarbij ingespeeld wordt op toekomstige commerciële wensen door optimaal gebruik te maken van technologische mogelijkheden binnen het kader van sociale en economische randvoorwaarden. Gekozen is voor een geleidelijke transformatie in zeven jaar (1990-1997) om de noodzakelijke veranderingen binnen het kernbedrijf van de Postbank bestuurbaar en beheersbaar te houden. Na afronding van het overleg met de Ondernemingsraad zal een definitief besluit worden genomen over de invoering van het nieuwe verwerkingsproces.

3 Het nieuwe verwerkingsproces

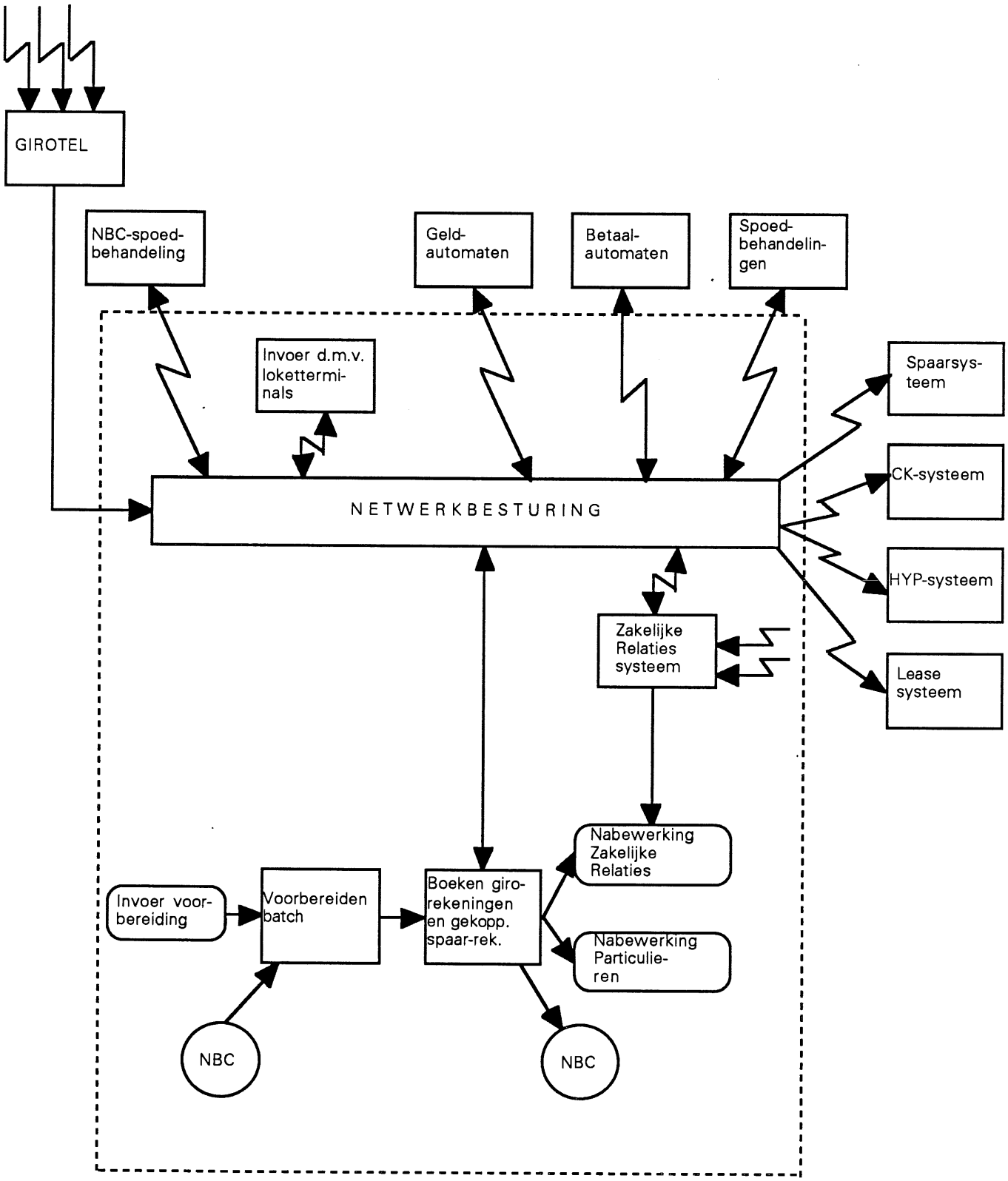
3.1 Algemeen

Uitgebreid is onderzocht hoe het nieuwe verwerkingsproces ingericht zou moeten worden. Hierbij is veel aandacht besteed aan het inventariseren van de eisen en wensen waaraan het verwerkingsproces van het betalingsverkeer in de toekomst moet voldoen. Deze eisen zijn gebaseerd op te verwachten aantallen transacties, soorten produkten en verwerkingstijden.
Het nieuwe verwerkingsproces omvat:
- de boekingsfunctie;
- de invoer, uitvoer en documentaanmaak;
- de zakelijke relaties verkeersprocessen;
- elektronisch betalingsverkeer en invoer door middel van loket-terminals.

In verband met de nauwe relatie met het verwerkingsproces wordt tevens het beheer van de cliëntgegevens en het bewaken van het gebruik van de girorekeningen bij de vernieuwing betrokken.

Schematisch is in figuur 2 weergegeven welke gebieden tot het nieuwe verwerkingsproces behoren. Dat zijn alle aspecten die binnen de stippellijn vallen. Buiten het nieuwe verwerkingsproces

vallen Girotel, Consumptief Krediet, Hypotheken, Betaal- en Geldautomaten etc.
De interfaces met deze systemen behoren wel tot het nieuwe verwerkingsproces.



Figuur 2

3.2 Randvoorwaarden en uitgangspunten van het nieuwe verwerkingsproces

De randvoorwaarden betreffen voorwaarden die de omgeving aan het nieuwe verwerkingsproces stelt. Bij het realiseren van het nieuwe verwerkingsproces moet onvoorwaardelijk aan deze voorwaarden worden voldaan. Zij zijn afgeleid uit besluiten van de Raad van Bestuur, het Strategisch Plan Postbank 1988-1995 en de bedrijfsplannen van de bedrijfsonderdelen van de Postbank.
Enkele belangrijke randvoorwaarden zijn:
- de eisen die geformuleerd zijn in het statuut "Betrouwbaarheid en continuïteit (geautomatiseerde) gegevensverwerking Postbank N.V.";
- de eisen die geformuleerd zijn in het privacy reglement "Cliëntenadministratie Postbank N.V.";
- eisen die voortvloeien uit sociale, organisatorische en economische aspecten.

Uitgangspunten zijn realisatiecondities die in afstemming met het operationele en functionele management voor het verwerkingsproces zijn gedefinieerd.
Het aantal uitgangspunten is zeer talrijk en is gegroepeerd naar de aandachtspunten effectiviteit, efficiency, flexibiliteit, continuïteit en betrouwbaarheid.
Voor de beeldvorming van het nieuwe proces wordt er onderstaand een aantal ter illustratie weergegeven.

Ten aanzien van de effectiviteit:
- de bestaande functionaliteit van het huidige verwerkingsproces voor particuliere en zakelijke relaties dient in het nieuwe proces te worden overgenomen;
- het verwerkingsproces dient zowel batch-verwerking als real time-verwerking te kunnen uitvoeren;
- de zakelijke klant moet op één punt in de Postbankorganisatie terecht kunnen voor al zijn (betaal)zaken;
- het verwerkingsproces moet 24 uur per dag, zeven dagen in de week beschikbaar zijn met een gegarandeerde beschikbaarheid van minimaal 99%;
- het voorbereidings- en afhandelingssysteem ten behoeve van het elektronisch betalingsverkeer moet 24 uur per dag, zeven dagen in de week beschikbaar zijn met een gegarandeerde beschikbaarheid van minimaal 99,95%.

Ten aanzien van de efficiency:
- de kosten van de verwerking van de standaardbetalingsopdrachten moeten verder omlaag;
- het invoerproces voor de verwerking van de massale standaardopdrachten en de verwerking van de betaalopdrachten dient verdergaand te worden geautomatiseerd.

Ten aanzien van de flexibiliteit:
- het nieuwe verwerkingsproces dient snelle capaciteitsgroei van het elektronisch betalingsverkeer en verschuivingen van "document" betalingsverkeer naar "elektronisch" betalingsverkeer flexibel en snel te kunnen opvangen;
- het nieuwe verwerkingsproces moet flexibel en toekomstvast zijn. Bij introductie van nieuwe produkten moeten namelijk geen of zo min mogelijk wijzigingen plaatsvinden;
- de hoofdfuncties uit het huidige verwerkingsproces dienen te worden ontvlochten tot afzonderlijke systeemdelen. Interfaces tussen de afzonderlijke systeemdelen en naar externe systemen dienen afzonderlijk te worden onderkend en gedefinieerd.

Ten aanzien van de continuïteit:
- voor het verwerkingsproces, inclusief de bijbehorende voorbereidings- en afhandelingssystemen geldt, indien noodzakelijk, dat de externe uitwijk bij calamiteiten binnen 48 uur gerealiseerd moet kunnen worden. De interne uitwijk moet voor de in verband met de continuïteit essentiële systeemdelen binnen enkele minuten gerealiseerd zijn;
- voor het systeem ten behoeve van het elektronisch betalingsverkeer geldt dat de externe uitwijk binnen enkele seconden gerealiseerd moet kunnen worden. (Onder interne uitwijk wordt verstaan uitwijk naar een back-up-computer binnen het desbetreffende computercentrum.

Externe uitwijk is de uitwijk naar een back-up-computer die staat opgesteld in een computercentrum op een andere geografische locatie.)

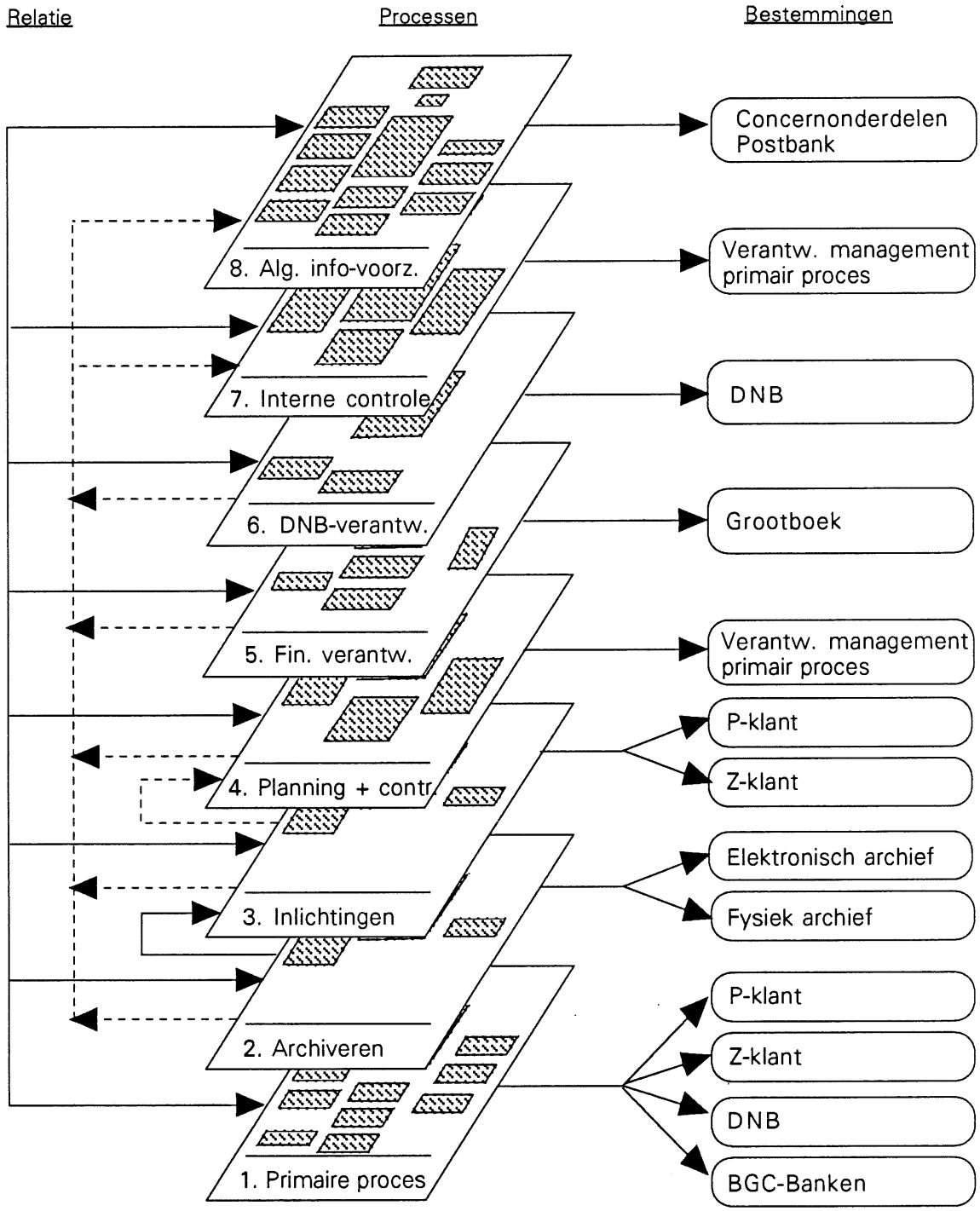
Ten aanzien van de betrouwbaarheid:
- het verwerkingsproces en de daaraan gerelateerde informatiesystemen moeten voldoen aan de eisen voor beheersbaarheid, betrouwbaarheid en controleerbaarheid die het verantwoordelijk management stelt;
- het verwerkingsproces mag niet over mogelijkheden beschikken om zelf boekingstransacties te genereren;
- het mag niet mogelijk zijn dat de klant zelf boekingen door middel van een terminal rechtstreeks aan het boekingssysteem aanbiedt en laat uitvoeren. Wel dient het mogelijk te zijn dat de klant transacties kan aanbieden aan architectuurdelen, die deze transacties dan onder eigen verantwoordelijkheid weer aanbieden aan het verwerkingsproces (bijvoorbeeld Girotel);
- er dient bij transacties die via terminals worden aangeboden, eenduidig te worden bepaald op welke momenten de controleverantwoordelijkheid en de financiële aansprakelijkheid van de ene op de andere partij overgaat.

3.3 Systeemarchitectuur van het nieuwe verwerkingsproces

De verschillende systeemdelen van het nieuwe verwerkingsproces dienen zo onafhankelijk mogelijk te kunnen functioneren om een optimale flexibiliteit te garanderen. Dit is noodzakelijk om wijzigingen en aanvullingen op systeemdelen te kunnen doorvoeren zonder dat alle systeemdelen in beschouwing moeten worden genomen, dan wel moeten worden gewijzigd. Daartoe zijn bij het definiëren van de voorgestelde architectuur twee principes gehanteerd, te weten:
- specialisatie, of wel splitsing naar processen;
- differentiatie, of wel splitsing naar processtappen.

Specialisatie

Het principe van specialisatie heeft - rekening houdend met gestelde randvoorwaarden en uitgangspunten - geleid tot de achtlagenstructuur welke in figuur 3 is weergegeven.
Binnen deze lagenstructuur is een splitsing gemaakt tussen het primaire proces Betalen en de secundaire processen Betalen. Per architectuurlaag worden hierin de relaties met het primaire proces, alsmede de processen en de bestemmingen van de uitvoer van deze processen beschreven.



Figuur 3

Het primaire proces Betalen vormt de kern van het verwerkingsproces (de "fabriek" van de Postbank) en verzorgt een gecontroleerde verwerking en afhandeling van betaaltransacties: het verplaatsen van "geld" en het bijhouden van het saldo en vaste gegevens van de girorekening. In dit proces zijn de controles op de verschillende processtappen, de procescontroles, geïntegreerd. Door middel van deze procescontroles wordt gewaarborgd dat de gegevens die de "fabriek" ingaan en de gegevens die de "fabriek" uitgaan juist, volledig, tijdig en geautoriseerd verwerkt zijn.

De secundaire processen dienen voor de verantwoording en besturing van het primaire proces en voor het verschaffen van informatie over het primaire proces. Deze secundaire processen zijn op hun beurt naar de diverse onderwerpen gespecialiseerd, te weten:
- archiveren;
- inlichtingen;
- planning en control;
- financiële verantwoording;
- verantwoording aan De Nederlandsche Bank (DNB);
- interne controle;
- algemene informatievoorziening.

Zolang geen nieuwe gegevens uit het primaire proces nodig zijn voor wijzigingen en aanvullingen in de secundaire processen, kunnen deze wijzigingen onafhankelijk van het primaire proces worden uitgevoerd. De gegevensbeheerfunctie zal echter het raadplegen dan wel het kopiëren van de gegevens moeten autoriseren.

Wannneer voor wijzigingen en aanvullingen in de secundaire processen nieuwe gegevens uit het primaire proces nodig zijn, zullen deze in het primaire proces moeten worden vastgelegd. Vervolgens dienen deze gegevens te worden overgedragen aan de secundaire processen.

Hieruit blijkt de begrenzing van de onafhankelijkheid tussen het primaire proces en de secundaire processen. Een behoefte aan nieuwe, nog niet eerder vastgelegde, gegevens zal effecten hebben op het primaire proces, maar zolang dat niet het geval is, zijn de secundaire processen volkomen onafhankelijk en dus flexibel.

Differentiatie

Het principe van differentiatie is toegepast op het primaire proces. Dit heeft geleid tot opsplitsing in een vijftal systeemgebieden:
Invoer, Operations, Uitvoer, Rekeningbeheer en -bewaking en Zakelijke verkeersprocessen.
Het uitgangspunt hierbij is dat elk systeemgebied zelf kan bepalen wat er met de te verwerken invoer moet gebeuren en wanneer en hoe dat gebeurt. De enige koppeling tussen de systeemgebieden is de transactie-overdracht. Elk systeemgebied dat een transactie aanneemt van een ander systeemgebied is zelf verantwoordelijk voor de verwerking daarvan. Vervolgens is binnen deze systeemgebieden weer het specialisatieprincipe toegepast.

Dit resulteert in een onderscheid tussen onder meer:
- batch- en real time-verwerking;
- automatische en handmatige conversie;
- zakelijk en particulier cliëntenbeheer;
- NBC- en Postbankverkeer.

Het fundament van de informatie- en systeemarchitectuur wordt gevormd door het primaire proces. In deze architectuurlaag zijn alle functies gedefinieerd die noodzakelijk zijn voor het verwerken van betaaltransacties. Naast procescontroles bevat deze laag tevens voorzieningen die zorg dragen voor een optimale informatie-uitwisseling met de secundaire processen. Dit laatste is zichtbaar gemaakt in figuur 3 door middel van de zeven lagen van de secundaire processen boven de architectuurlaag van het primaire proces.

De indeling van de primaire architectuurlaag in systeemgebieden is op het niveau van de secundaire processen voor zover relevant gehandhaafd. Dit maakt het mogelijk om wanneer een systeemdeel wordt ontwikkeld, tegelijkertijd de "bovenliggende" secundaire processen te ontwikkelen en toch de functionele onafhankelijkheid te handhaven. Gezien vanuit de doelstelling van dit artikel wordt in hoofdstuk 4 verder ingegaan op laag 7 van het model "het proces interne controle".

3.4. Organisatie ten behoeve van de vernieuwing van het verwerkingsproces

Gezien de aard en complexiteit van het project, vernieuwen van het operationele verwerkingsproces, en de geplande lange realisatieduur kon niet worden volstaan met een projectorganisatie of een zuivere matrixorganisatie waarin alleen medewerkers van de huidige directoraten en concerneenheden deelnemen.
Geschat wordt dat voor het managen, de bouw en de implementatie 1.300 mensjaar benodigd zullen zijn en dat de totale investering *f* 985 miljoen zal bedragen (inclusief anders noodzakelijke vervangings/uitbreidingsinvesteringen). De vernieuwing zal in deels parallel verlopende trajecten worden gerealiseerd. Binnen die trajecten worden projecten gedefinieerd, opgestart en gerealiseerd.

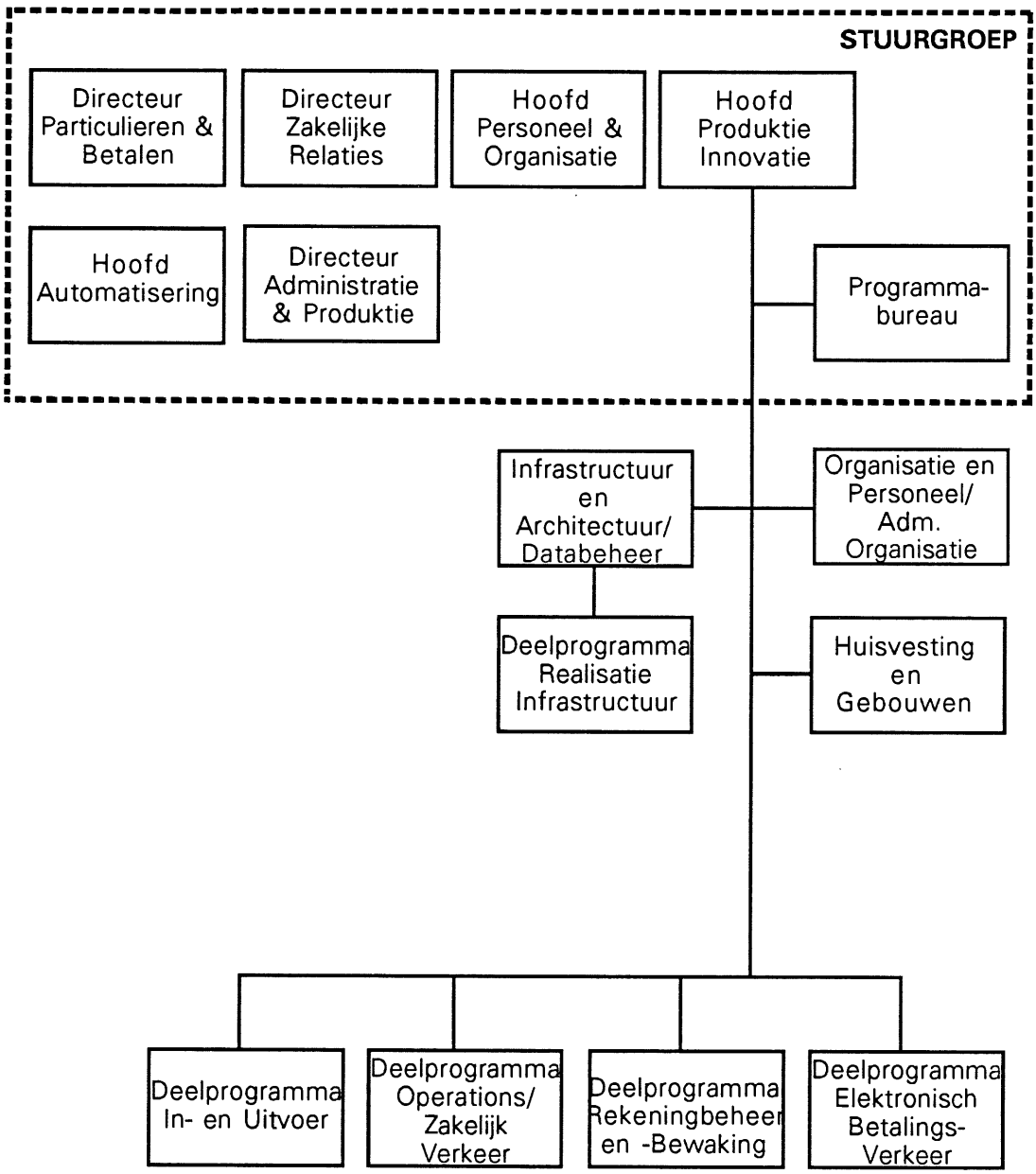
Om de noodzakelijke aandacht te kunnen besteden aan dit omvangrijke en kritieke projectenprogramma en om eenduidig de verantwoordelijkheid van de Raad van Bestuur voor de voortgang en de realisatie van een nieuw verwerkingsproces te kunnen aangeven, is besloten een tijdelijke organisatie met een vaste bemensing direct onder de Raad van Bestuur in het leven te roepen.
Binnen de Postbank heet deze tijdelijke organisatie "Produktie-Innovatie" of kortweg PI.

Overigens betekent dit niet dat alleen de vaste bemensing zal werken aan de realisatie van het programma.
Het totale programma zal worden verdeeld in deelprojecten, die door projectgroepen zullen worden uitgevoerd, waarin zowel medewerkers van Produktie-Innovatie als medewerkers van de directoraten en overige concerneenheden deelnemen.

De medewerkers van de directoraten en de andere concernonderdelen die bij de deelprojecten worden ingeschakeld (waarbij met name aan personeel van de concerndienst Automatisering moet worden gedacht), blijven ingedeeld bij hun oorspronkelijk onderdeel. Na afloop van hun activiteiten in de projecten van het programma Produktie-Innovatie gaan zij weer terug naar hun onderdeel.

Voor de beleidsvoorbereiding is een stuurgroep opgericht, waarin naast een lid van de Raad van Bestuur en de leiding van Produktie-Innovatie tevens de directeuren en hoofden van de betrokken concernonderdelen zitting hebben.
Het hoofd van de Interne accountantsdienst is lid op ad hoc-basis.

De inrichting van Produktie-Innovatie is in figuur 4 weergegeven. Als taakstelling voor Produktie-Innovatie is geformuleerd:
- het definiëren van een nieuw verwerkingsproces dat voldoet aan de eisen van effectiviteit, efficiency, flexibiliteit, continuïteit en betrouwbaarheid;
- het opstellen van samenhangende plannen voor de invoering van het nieuwe verwerkingsproces voor informatica, personeel, organisatie en huisvesting;
- het voorbereiden van de uitvoering van de samenhangende plannen voor vernieuwing;
- het coördineren en beheersen van de realisatie en ingebruikneming van het nieuwe verwerkingsproces mede in relatie tot de lopende ontwikkelingen in het betreffende gebied. De acceptatie en de feitelijke invoering van het nieuwe verwerkingsproces geschieden onder verantwoordelijkheid van de staande organisatie.



Figuur 4

4 Interne controle en beveiliging

4.1 Algemeen

Binnen een project als PI is het van groot belang dat in een zo vroeg mogelijk stadium expliciet aandacht wordt besteed aan de opzet en de beschrijving van de interne controlestructuur.
Onder een dergelijke structuur dient in dit kader te worden verstaan: een samenhangend geheel van interne controle- en beveiligingsmaatregelen in en rond het verwerkingsproces, gericht op de beheersbaarheid, de betrouwbaarheid en de controleerbaarheid van de feitelijke bedrijfsvoering.

Het doel van de beschrijving van de interne controlestructuur is, uitgaande van een risico-analyse, te komen tot een evenwichtig pakket van maatregelen van interne controle en beveiliging zonder dat er witte vlekken of doublures optreden.
De beschrijving van deze structuur dwingt tot een expliciete bezinning op deze maatregelen en tot een integratie in het totale systeemconcept door het opnemen van meet-, beslis- en controlepunten. Gelijktijdig ontstaat daardoor een instrument voor het management voor de beheersing van de bedrijfsvoering.

De interne controlestructuur vormt hét instrument waarmee het management de beheersbaarheid, de betrouwbaarheid en de controleerbaarheid van de bedrijfsvoering kan waarborgen. Het is dan ook primair de verantwoordelijkheid van dit management zorg te dragen voor het opzetten en invoeren van een evenwichtig stelsel van interne controle- en beveiligingsmaatregelen.

Om tot een evenwichtige samenstelling van maatregelen te komen moet, door de projectorganisatie, eerst worden onderzocht aan welke risico's het systeem is onderworpen.
Aan de hand daarvan zal binnen het kader van de systeemeisen een opstelling moeten worden gemaakt van interne controle- en beveiligingseisen.

Het is een beslissing van het lijnmanagement om aan de hand van de geformuleerde eisen en de gesignaleerde risico's te bepalen welke maatregelen, preventief dan wel detectief of correctief van aard, zullen worden getroffen.

De IAD/Postbank heeft binnen het programma Produktie-Innovatie een adviserende, signalerende en bewakende taak ten aanzien van:
- de vereiste controlemaatregelen in het verwerkingsproces;
- de vereiste controleprocedures in de organisatie rond het verwerkingsproces;
- de afstemming van geautomatiseerde en procedurele controlemaatregelen binnen het verwerkingsproces alsmede de afstemming met maatregelen die in andere aansluitende systemen zijn genomen.

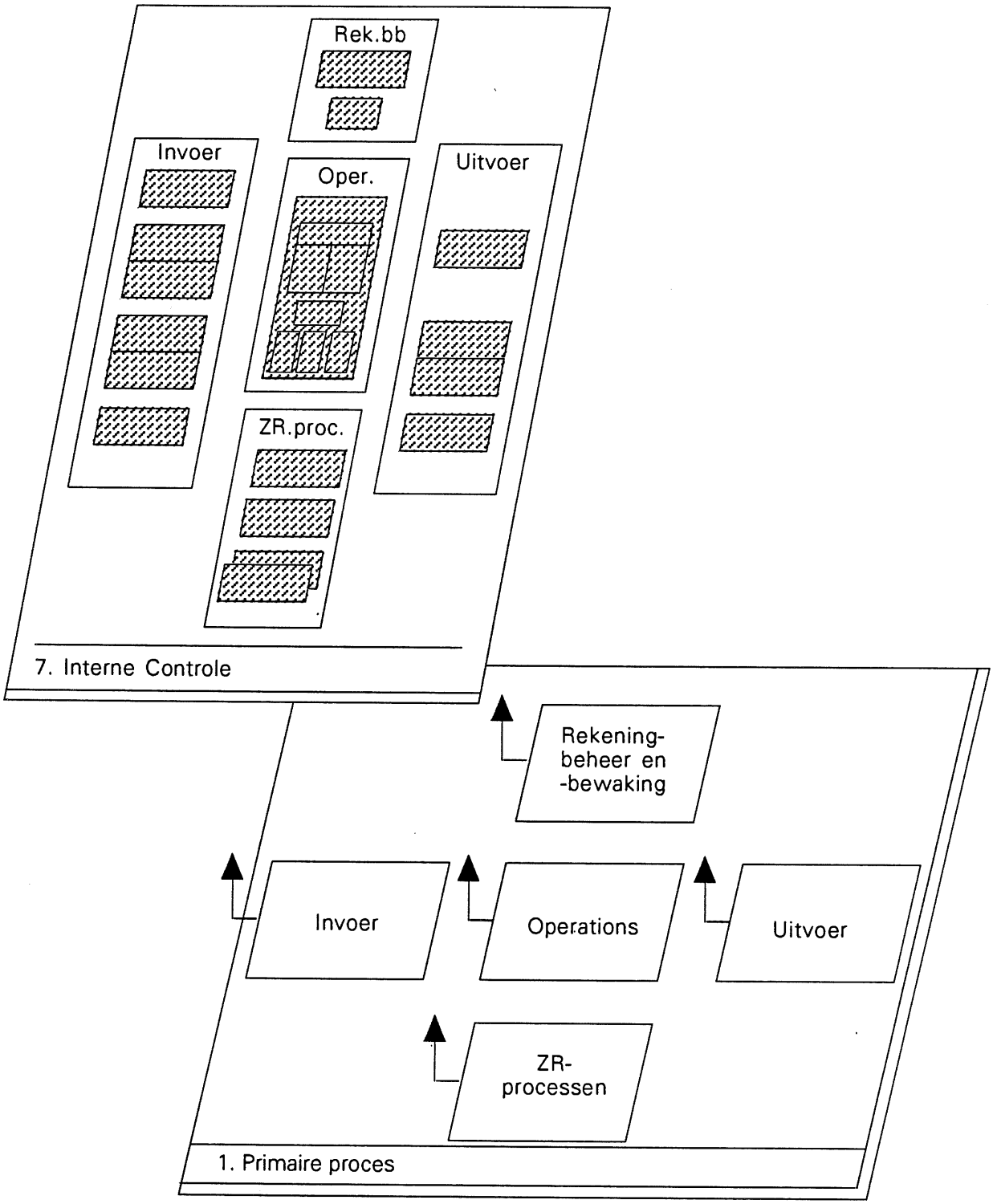
Om dit te operationaliseren heeft de IAD bij de start van de vernieuwing van het verwerkingsproces interne controle- en beveiligingseisen gesteld. De geformuleerde eisen zijn van een relatief hoog abstractieniveau. Dit is gedaan ten behoeve van algemene geldigheid voor alle binnen het verwerkingsproces onderkende processen.

De door de IAD/Postbank in de planvormingsfase van Produktie-Innovatie gestelde eisen hebben betrekking op:
- de beheersing van de systeemontwikkeling;
- de beheersing van het verwerkingsproces onderverdeeld in algemene eisen en specifieke eisen betreffende de invoer, verwerking, opslag en uitvoer van gegevens;
- de netwerkbesturing.

4.2 Interne controle- en beveiligingsstructuur

Een eerste opzet van de interne controlestructuur heeft in algemene termen plaatsgevonden aan de hand van het globale systeemconcept van het nieuwe verwerkingsproces en de door de IAD opgestelde interne controle- en beveiligingseisen.
Dit heeft onder andere geresulteerd in een aantal uitgangspunten voor het nieuwe verwerkingsproces (zie 3.2).
De globale interne controlestructuur moet binnen de onderscheiden deelprojecten op basis van nadere voor de desbetreffende deelprojecten op te stellen risico-analyses verder uitgewerkt worden. Noodzakelijk hiervoor is onder andere dat besluitvorming heeft plaatsgevonden ten aanzien van:
- welke automatiseringstechnieken zullen worden toegepast;
- hoe de verwerkingsorganisatie er komt uit te zien;
- hoe de gebruikersorganisatie gestructureerd gaat worden.

In samenvattende vorm zal de interne controlestructuur van het verwerkingsproces er als volgt gaan uitzien (zie figuur 5):



Figuur 5

a. Uitgangspunten zijn de vijf deelprocessen van het primaire proces te weten:
   - invoer;
   - boeken (operations);
   - uitvoer;
   - rekeningbeheer en -bewaking;
   - zakelijke verkeersprocessen.

   Door middel van procescontroles (dit is een uitgebreid stelsel van geprogrammeerde controles, zowel detailcontroles als verbandscontroles) wordt per deelproces gewaarborgd dat de

gegevens die het proces ingaan, verwerkt worden en uitgaan juist, volledig, tijdig en geautoriseerd zijn én blijven. Het balansevenwicht binnen het primaire proces wordt gerealiseerd door zowel voor de batch- als de on-line-mutaties consequent tweezijdig te boeken.

b. Het management dat verantwoordelijk is voor de primaire deelprocessen dient gegevens te laten vastleggen door deze processen waarmee de beheersbaarheid, de betrouwbaarheid en controleerbaarheid van het proces en dus de bedrijfsvoering gewaarborgd kan worden. De hierbedoelde informatie wordt vastgelegd in laag 4 "Planning en control" voor wat betreft stuurgegevens en in laag 7 "Interne controle" voor wat betreft controlegegevens (zie figuur 3). Het is niet de bedoeling dat de interne controle een zelfstandig proces is. Uiteraard is de interne controle geïntegreerd in alle (deel)processen. De specifiek voor de controle door het management benodigde informatie wordt vastgelegd in laag 7.

c. Als overkoepelende controle van het gehele verwerkingsproces wordt een netwerk van controletotalen gedefinieerd. Hiermee wordt periodiek de integriteit van de saldi database vastgesteld. Tevens is dit het controlemiddel om bij reconstructie van de database de juistheid en volledigheid van de in de database opgeslagen gegevens te kunnen vaststellen.
Het netwerk van controletotalen wordt geregistreerd in laag 7 "Interne controle". Hiertoe wordt het totale rekeningenbestand in een aantal groepen onderverdeeld.
Per groep rekeningnummers wordt hierin onder andere opgenomen:
   - de som van de rekeningnummers;
   - de som van de saldi;
   - de som van de "af-" respectievelijk "bij"-mutaties vanuit de batch-invoerprocessen voor de te bewaken gegevens;
   - de som van de "af-" respectievelijk "bij"-mutaties vanuit de on-line-invoerprocessen voor de te bewaken gegevens.

   Periodiek wordt per groep rekeningnummers geverifieerd of de met behulp van bovengenoemde elementen berekende eindstand van de som van de rekeningnummers en saldi overeenstemt met de actuele database uit het primaire proces.

d. Het management dat informatie uit de primaire processen gebruikt, bijvoorbeeld Financiële Zaken (zie laag 5 uit figuur 3), is zelf ook weer verantwoordelijk voor het creëren van een adequate interne controle- en beveiligingsstructuur ter waarborging van de beheersbaarheid en controleerbaarheid van de bedrijfsvoering van het desbetreffende secundaire proces.

5 Samenvatting

De vernieuwing van het verwerkingsproces van het betalingsverkeer draagt ertoe bij dat de Postbank ook in de toekomst een gratis basispakket voor betalingsfaciliteiten ter beschikking van haar cliënten kan stellen.
Daarnaast wordt het mogelijk aan cliënten naast de bestaande standaarddiensten meer faciliteiten te bieden. Te denken valt hierbij onder andere aan agenderen, reserveren en saldoregulatie.
Tevens wordt het vanwege de modulaire opzet van het nieuwe verwerkingsproces, door het in verregaande mate toepassen van het specialisatie- en differentiatieprincipe, mogelijk het systeem snel en efficiënt aan te passen aan de steeds wisselende omstandigheden en nieuwe eisen. Een hoog niveau van betrouwbaarheid en controleerbaarheid wordt gerealiseerd door vanaf het eerste stadium expliciet aandacht te schenken aan interne controle- en beveiligingsaspecten, zodat de interne controle- en beveiligingsstructuur een geïntegreerd ontwerpcriterium wordt.
Met het nieuwe verwerkingsproces van de Postbank zal de NMB Postbank Groep haar dominante positie in het betalingsverkeer verder kunnen uitbouwen.

MOGELIJKHEDEN TOT STANDAARDISATIE VAN DE BEVEILIGING VAN GEAUTOMATISEERD GIRAAL BETALINGSVERKEER

door drs. A. Hemelaar RA, adjunct-directeur BankGiroCentrale

Het girale betalingsverkeer vervult een wezenlijke functie in de moderne maatschappij. Het is in de laatste decennia uitgegroeid tot een breed pakket van veelal geautomatiseerde faciliteiten, waarbij gebruik kan worden gemaakt van media als magneetband, diskette en datacommunicatie.
Elektronisch betalen in brede zin is gemeengoed geworden voor zowel particulieren als bedrijven en instellingen.
Het blijkt dat door allerlei ontwikkelingen de traditionele beveiligingsmethoden niet meer adequaat zijn. Nieuwe geautomatiseerde beveiligingsmethoden zijn en worden dan ook ontwikkeld. Gezien het massale karakter van betalingsverkeer is standaardisatie daarbij noodzaak.

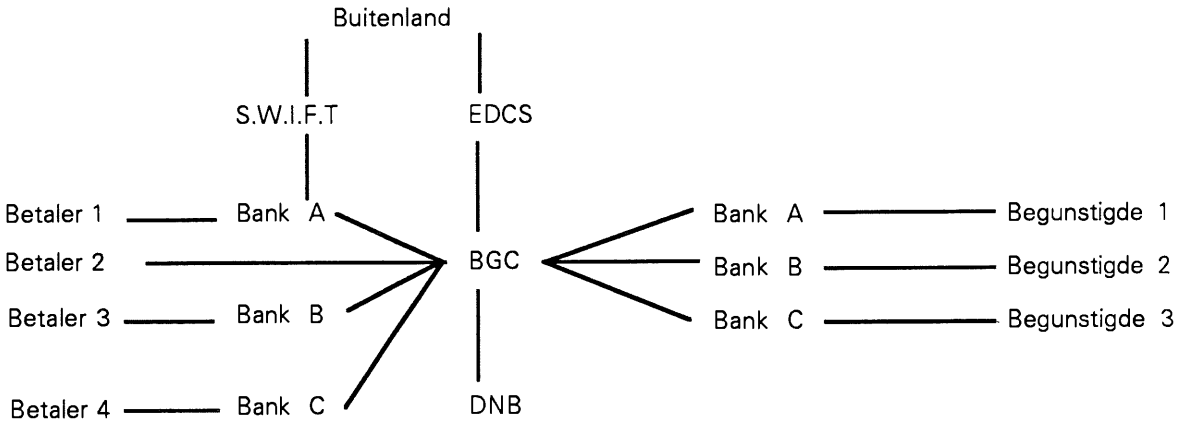
Giraal betalingsverkeer

Giraal betalingsverkeer kan worden beschouwd als een systeem waarin gebruikers - cliënten van de banken - onderling vorderingen en schulden verrekenen door af- en bijschrijvingen op bij banken aangehouden rekeningen.

In dit systeem werken verschillende partijen samen.
De meest eenvoudige situatie is de betaling via één bank; de loop van de betaling daarbij is als volgt: Betaler - Bank - Begunstigde.
Deze situatie doet zich voor wanneer betaler en begunstigde hun rekening bij dezelfde bank hebben. De berichtenstroom gaat meestal van betaler naar begunstigde. Bij incasso (machtigen) gaat de stroom in tegenovergestelde richting. Bij elektronisch betalen door particulieren is er sprake van een dialoog met de bank in verband met de geautomatiseerde autorisatie en de verificatie van de PIN-code. Met andere woorden: er is geen éénrichtingsverkeer op de trajecten. Deze opmerking geldt eveneens voor de hierna te beschrijven complexere situaties.

In de meeste gevallen echter is het systeem complexer.
Bedrijven en instellingen leveren opdrachten vaak aan bij de BankGiroCentrale (BGC) en bij verscheidene banken. De banken zenden opdrachten door naar de BGC, namelijk die welke bij een andere bank moeten worden gecrediteerd of gedebiteerd.
De BGC zorgt voor het doorgeven van de berichten.
De netto te verrekenen bedragen worden via De Nederlandsche Bank (DNB) verevend. Bovendien is er ook financieel berichtenverkeer van en naar het buitenland. Voor het zakelijk verkeer loopt dit via S.W.I.F.T. (Society for Worldwide Interbank Financial Telecommunication). Voor particulieren die over de grens elektronische transacties verrichten wordt gebruik gemaakt van EDCS (European Payment Systems Services Data Communication System).

Het schema wordt nu als volgt:

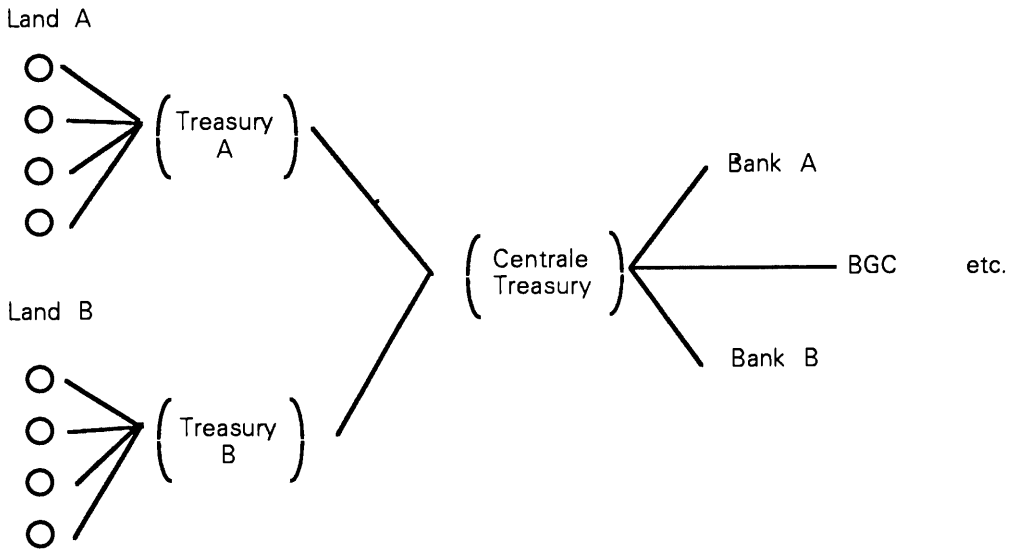


Wanneer een particuliere cliënt in Spanje bij een automaat geld opneemt of betaalt via een betaalautomaat, benadert hij zijn bank dus via het EDCS-netwerk.

Wat S.W.I.F.T. betreft beschikken de grote banken over een eigen terminal van het SWIFT-netwerk.

Bij grote concerns met een centrale treasury-afdeling is de situatie nog gecompliceerder. Vaak is er sprake van concern-verrekeningen en/of worden bepaalde betalingen via de treasury-afdeling geleid, bijvoorbeeld die aan het buitenland.
Voordat een bericht bij de bank komt, gaat er dus een concern-berichtenverkeer aan vooraf.
Bij multinationals kan er sprake zijn van zowel een landelijke als een centrale treasury-afdeling.

Dit blijkt uit het volgende schema:

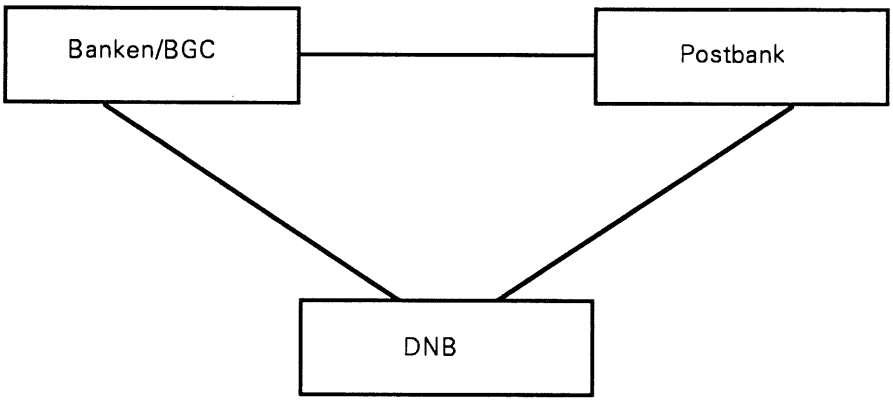


Concluderend kan worden vastgesteld dat betalingsverkeer een systeem is waarbij massaal berichtenverkeer zich voltrekt over een groot aantal trajecten tussen veelal onafhankelijke partijen. Uit dien hoofde is standaardisatie van het berichtenverkeer en eveneens van de beveiliging noodzaak.

Bepalend voor de werkwijze (infrastructuur) van een giraal betalingssysteem zijn de banken. Deze zijn verantwoordelijk voor de technische en procedurele infrastructuur.

Wanneer een aantal banken samenwerkt om de vormgeving van het betalingsverkeer te uniformeren - standaardiseren zo men wil - dan ontstaat een zogenaamd betalingscircuit. In Nederland is er het **circuit van de bij de BankGiroCentrale aangesloten banken**. De Postbank doet daaraan niet mee; deze heeft haar eigen methoden en technieken. Om die reden spreekt men ook wel van het **Postbankcircuit**. Daarnaast is er nog het **topgirocircuit** van De Nederlandsche Bank, waar de banken hun vorderingen en schulden onderling verrekenen (verevenen).

Schematisch kunnen de circuits als volgt worden voorgesteld:



Betalingsverkeer tussen verschillende circuits kost vanwege de nodige aanpassing van de berichten bij de "grensoverschrijding" extra inspanning, hetgeen een langere tijdlijn tussen debiteuren en crediteuren tot gevolg kan hebben. Vandaar dat in Nederland gestreefd wordt naar één **Nationaal Betalings Circuit**.

Beveiliging

Noodzaak van beveiliging

Financieel berichtenverkeer is een kernfunctie in het nationale en internationale economische systeem. Het is onbetwistbaar dat betalingsfaciliteiten bij voortduring ter beschikking moeten staan en dat het berichtenverkeer een hoge mate van betrouwbaarheid moet hebben.

In dit artikel wordt het focus niet gericht op de beschikbaarheid, maar op de betrouwbaarheid. Betrouwbaarheid omvat hier de elementen:
- authenticiteit;
- rechtmatigheid (geoorloofdheid);
- integriteit.

Het moet duidelijk en bewijsbaar zijn wie de opdracht verstrekt (authenticiteit), dat de betaler gerechtigd is om de opdracht te verstrekken (geoorloofdheid) en dat de gegevens van de opdracht niet veranderd zijn na de initiële vaststelling (integriteit).

Vertrouwelijkheid heeft in het betalingsverkeer niet die hoge prioriteit als bijvoorbeeld bij militaire informatie. Wel hebben bankfunctionarissen de plicht tot geheimhouding, omdat sommige betalingen van vertrouwelijke aard zijn. Dit geldt bijvoorbeeld voor persoonlijke inkomens. Ook kunnen saldi van rekeningen als vertrouwelijke gegevens worden aangemerkt. Toch wordt versluiering van deze gegevens slechts in weinig gevallen toegepast. Meestal is een goede toegangsbeveiliging - die tevens nodig is in verband met het waarborgen van de integriteit - voldoende.

Giraal betalen heeft mede zo'n grote vlucht genomen omdat het een veilig systeem is. Door de administratieve vastlegging van de processen is er altijd een audit-trail.
Indien er fouten worden gemaakt - die overigens relatief zeer gering zijn - dan kunnen die zonder al

te grote bezwaren weer worden teruggedraaid. Wil men frauduleus gelden aan het circuit onttrekken, dan is dit wanneer het om grote bedragen gaat, niet gemakkelijk. Om deze redenen kon het systeem ook in geautomatiseerde vorm vele jaren functioneren met een hoge graad van betrouwbaarheid.

De laatste jaren nemen de bedreigingen echter toe:
- het gebruik van datacommunicatie betekent dat het aantal toegangen tot de systemen, vaak in een niet gecontroleerde omgeving, aanzienlijk toeneemt;
- er is een trend naar volcontinue service waardoor rustpunten in de verwerking wegvallen; corrigeren tijdens de verwerkingen of achteraf is niet altijd meer mogelijk;
- de kennis van automatisering wordt steeds verder verspreid. Dit betekent dat ook de kennis van het manipuleren van de processen toeneemt;
- het gevaar bestaat dat de professionele criminaliteit zich gaat richten op het inbreken in financiële circuits.

Een beleid dat zich bezighoudt met de toekomst zal dan ook met deze factoren rekening moeten houden, met andere woorden: een goed beveiligingsbeleid is noodzaak.

Eisen te stellen aan beveiliging

Beveiliging is een kwaliteitsaspect van het produkt Betalingsverkeer. De mate van beveiliging is altijd een compromis tussen een aantal overwegingen:
1. de beveiliging moet **effectief** zijn in die zin dat de cliënt erop kan vertrouwen dat zijn opdrachten correct worden uitgevoerd en dat zijn rekening niet ten onrechte wordt belast;
2. de beveiligingsmaatregelen moeten zodanig **gebruikersvriendelijk** zijn dat ze door de gebruikers worden aanvaard;
3. de beveiligingsmaatregelen moeten **betaalbaar** zijn;
4. aangezien betalingsverkeer een aantal partijen aangaat, zullen deze het eens moeten worden over **uniforme** (gestandaardiseerde) beveiligingsmethoden.

Met name de laatste eis kan van invloed zijn op de voorgaande. In het vervolg zal daarop dan ook nog teruggekomen worden.

Trajecten en verwerkingsstations

De betalingsinformatie wordt geïnitieerd door de opdrachtgever, overgedragen ter verwerking aan een financiële instelling, weer doorgegeven enz. Er zijn dus verschillende verwerkingsstations en trajecten waarop de overdracht plaatsvindt van het ene naar het andere station.

De verschillende financiële instellingen hebben vaak verschillende fabrikaten en typen computerapparatuur en software, die elk weer verschillende mogelijkheden bieden voor de beveiliging van de verwerking. Deze mogelijkheden zijn meestal leverancier-(hardware)-gebonden en dan ook niet gestandaardiseerd. Aangezien er echter wel een algemene opvatting bestaat over de te stellen eisen, bieden de beveiligingspakketten vaak dezelfde functionaliteit en is er toch sprake van enige standaardisatie. Elke partij zal dus de beveiliging van de interne verwerking zelf moeten regelen. Aangezien de berichtenstroom de verschillende partijen passeert, dient de standaardisatie betrekking te hebben op de berichten (inhoud en indeling) en op de overdracht (het transport) van die berichten van de ene aan de andere partij.
De standaards voor beveiliging zijn dan ook gericht op de overdracht van de berichten, met andere woorden: op het traject tussen twee verwerkingsstations.

Beveiliging van trajecten

Het blijkt dat de eisen en mogelijkheden voor de beveiliging op verschillende soorten trajecten niet altijd dezelfde zijn.
Om deze reden wordt een aantal soorten trajecten onderscheiden, namelijk:
- de (initiërende) trajecten voorafgaand aan de opdrachtverstrekking aan de bank;
- de input-trajecten, te weten de opdrachtverstrekking;

- de trajecten tussen de financiële instellingen: de interbancaire uitwisseling;
- de output-trajecten, als de berichtgeving/verantwoording aan de cliënten.

Hierna worden deze trajecten nader bezien uit oogpunt van beveiliging.

Berichtenverkeer binnen bedrijven/concerns

Formeel behoren deze trajecten niet tot het bancaire betalingssysteem. Niettemin zijn de bancaire methoden van beveiliging toch van belang voor deze trajecten, omdat het voor de hand liggend is binnen de onderneming dezelfde methoden te hanteren. Als men bijvoorbeeld beschikt over een bancaire hash-functie[1] kan deze ook worden toegepast in de eigen crediteurenadministratie. En als er een systeem van elektronische handtekeningen met de bank is afgesproken, kan dit systeem ook worden toegepast binnen het concern. De keuzen van het bankwezen kunnen dus van belang zijn voor de individuele gebruikers/cliënten.

De trajecten van de opdrachtverstrekking

Hierbij moet onderscheid worden gemaakt tussen de geautomatiseerde opdrachtverstrekking door particulieren en die door zakelijke rekeninghouders. Er is namelijk een groot verschil tussen beide groepen rekeninghouders, hetgeen blijkt uit onderstaand overzicht (waarbij het Postbankcircuit buiten beschouwing is gelaten):

Aspecten	Elektronisch betalen en geld opnemen	Zakelijke betalings-transacties
Traject	Dialoog particulier-bank	Bedrijf naar bank of BGC
Geldstroom (schatting)	*f* 3 miljard	*f* 600 miljard
Aantal transacties (schatting)	20 miljoen (stijgt snel)	350 miljoen
Gemiddeld bedrag	*f* 150	*f* 1.700
Aantal deelnemers	3 miljoen	60.000
Kenmerken beveiliging	gebruikersvriendelijk, goedkoop, publicitair gevoelig	aanvaardbaar voor bedrijfsorganisatie, niet te duur

Gezien deze verschillen worden de beveiligingsaspecten hierna afzonderlijk behandeld.

Elektronische transacties van particuliere rekeninghouders

De beveiliging van de aanlevering van deze transacties bij de banken is geregeld: de pas met magneetstrip, gecombineerd met de geheime PIN-code geeft toegang tot de rekening. De pas, de gebruikte twee sporen op de magneetstrip en de toepassing van de PIN-code zijn gebaseerd op internationale standaards.
Weliswaar worden deze standaards niet overal - in de verschillende landen door de verschillende banken - op dezelfde wijze ingevuld, maar de basisconcepten zijn dezelfde. Daardoor is het mogelijk nationaal en internationaal gebruik te maken van geld- en betaalautomaten, een belangrijke faciliteit

1 Een hash-functie berekent op basis van de gegevens en met behulp van een algoritme een code, die de gegevens representeert. Met computerapparatuur kan deze code worden gebroken, doch dit vergt tijd. Een hash-functie beveiligt de gegevens dan ook gedurende een bepaalde periode.
Tot op heden worden bij de overdracht van een aantal betalingsopdrachten het totaal van de rekeningnummers en het totaalbedrag gebruikt als controlemiddelen. Door de hash-code worden deze vervangen.

voor de cliënten. Deze toegangsbeveiligingen worden ondersteund door de "achter" de apparatuur aanwezige infrastructuur. Zo wordt er bijvoorbeeld gebruik gemaakt van een interbancair autorisatienetwerk, met behulp waarvan de bank die de bankpas heeft verstrekt de transactie zelf kan controleren.

Ten aanzien van de gekozen oplossing wordt opgemerkt:
- dat de PIN-code in combinatie met de pas kan worden beschouwd als een persoonlijke elektronische handtekening[1], doch dat deze niet de integriteit van het bericht waarborgt. Hiervoor dienen (zijn) andere maatregelen. (Overigens is het gemiddelde bedrag van het bericht gering);
- dat de duurdere microcircuitkaart (chipkaart) uit oogpunt van beveiliging weliswaar voordelen heeft, doch de hoge prijs en de geringe beschikbaarheid van aangepaste apparatuur een massale toepassing vooralsnog onwaarschijnlijk maken.

Elektronische transacties van zakelijke rekeninghouders

Zakelijke cliënten verstrekken reeds sinds de oprichting van de BGC opdrachten die op geautomatiseerde wijze worden aangemaakt en aangeleverd. Hierbij kan worden gedacht aan opdrachten vastgelegd op magneetband en diskette, alsmede opdrachtverstrekking in de vorm van datacommunicatie.

Vanaf de jaren zeventig worden deze opdrachten beveiligd door gebruik te maken van een ondertekende opdrachtbrief met als controlemiddelen het totaalbedrag en een totaaltelling van de rekeningnummers. Een aantal cliënten zet bij deze controlemiddelen in het licht van de toekomstige ontwikkelingen een vraagteken; er wordt betwijfeld of de beveiliging op den duur voldoende zal zijn.

Gezien de verantwoordelijkheid van het bankwezen voor de vormgeving van het betalingsverkeer, dienen aan cliënten instrumenten verstrekt te worden, waarmee zij deze opdrachten beter kunnen beveiligen. Aangezien de ontwikkelingen op dit gebied nog gaande zijn, wordt er hierna wat dieper op ingegaan.

Voor dit traject zijn nog weinig of geen standaards beschikbaar. Er tekent zich echter wel een patroon af van de wijze waarop de beveiliging zal gaan plaatsvinden. Het blijkt namelijk dat het praktisch is de beveiliging op te delen in twee fasen:
- de toepassing van een hash-functie, die resulteert in wat wordt genoemd een "manipulation detection code". Deze code representeert de onderliggende gegevens;
- het plaatsen van een elektronische handtekening. Dit is een code die zowel de integriteit waarborgt van de gegevens als de authenticiteit van de inzender.

Het bankwezen in Nederland heeft sinds enige maanden de beschikking over een onderling afgesproken hash-functie die aansluit op een voorgestelde internationale standaard.
De hash-functie maakt gebruik van de Data Encryption Standard (DES) als algoritme; de hash-code die ontstaat na toepassing omvat 24 posities.
Deze 24 posities vertegenwoordigen gedurende een bepaalde periode onweerlegbaar de desbetreffende opdracht(en).

In de tweede fase wordt over de hash-code en enkele andere gegevens een zogenaamde elektronische handtekening gezet. De BankGiroCentrale heeft hiervoor een systeem ontwikkeld. Dit is gebaseerd op een chipkaart die een geheime sleutel bevat en functioneert als een security-module.
Het systeem werkt als volgt:
De chipkaart wordt ter beschikking gesteld aan een procuratiehouder, te zamen met een leesapparaat. De kaart wordt in het apparaat gestoken. De toegang tot de kaart is beveiligd met een PIN-code, die alleen aan de procuratiehouder bekend mag zijn. Nadat de hash-code is ingebracht in het apparaat (geautomatiseerd of met de hand ingetoetst) wordt de handtekeningcode berekend op basis van de ingebrachte gegevens en met behulp van de geheime sleutel en het DES-algoritme. Deze handtekeningcode wordt toegevoegd aan de opdracht.

---

1 In dit kader is de elektronische of digitale handtekening gedefinieerd als een code die door de betaler of veilige wijze in het systeem wordt ingebracht en die dient om de authenticiteit van de opdrachtgever vast te stellen.

Met deze handtekening wordt de integriteit gewaarborgd en de authenticiteit bij de huidige techniek praktisch onweerlegbaar vastgelegd.

Enige kanttekeningen:

- Het principe van beveiliging in twee fasen, ook wel genoemd twee lagen, wordt gebruikt in verschillende systemen die op de markt zijn.
  Er is echter verschil in de opvatting over de cryptografische techniek, met name wat betreft het gebruik van sleutels. Het BGC-systeem is gebaseerd op een symmetrisch algoritme. De sleutel voor de gebruiker wordt opgeborgen in een chipkaart; dit vereenvoudigt het sleutelbeheer en geeft een goede beveiliging. De(zelfde) sleutel wordt voor de controle in een centrale beveiligingsmodule opgeslagen.
  Er zijn echter ook voorstanders van asymmetrische algoritmes, zoals het RSA-algoritme. Zonder nu op deze plaats in te gaan op deze beide mogelijkheden - dit zou een uitgebreide technische toelichting vereisen - betekent dit verschil in opvatting dat er voorlopig nog geen algemene standaard mag worden verwacht.

- De hier beschreven systematiek werkt alleen op het traject cliënt-bank/BGC. Er wordt wel gepleit voor een "end-to-end" beveiliging waarbij verwerkingsstations op de weg van zender naar uiteindelijke ontvanger als het ware worden overbrugd.
  Dit betekent dat de partijen aan het begin en aan het eind van het proces een onderlinge sleutelrelatie moeten aangaan. Dit is wel mogelijk, maar op grote schaal praktisch moeilijk uitvoerbaar.

  De elektronische handtekening kan ook worden gebruikt voor toegangsbeveiliging. Een hash-code is dan niet nodig. De partij die toegang vraagt tot een systeem, bijvoorbeeld bij electronic banking, wordt daar op de volgende wijze geïdentificeerd:
  . de cliënt vraagt toegang;
  . de bank zendt een willekeurig gegeven toe;
  . de cliënt plaatst daarover zijn elektronische handtekening en zendt deze naar de bank;
  . deze controleert de handtekening en daarmee de identiteit van de zender.

Trajecten tussen de financiele instellingen

Het gaat hierbij om het doorgeven van berichten met betrekking tot het betalingsverkeer op de trajecten tussen banken c.q. tussen BGC en banken (inclusief Postbank). Deze stromen kunnen worden getypeerd door de volgende gegevens:

Geldstroom (schatting)	*f* 4.000 miljard
Aantal transacties (schatting)	1 miljard
Gemiddeld bedrag	*f* 4.000
Aantal deelnemers	circa 70
Kenmerken beveiliging	geautomatiseerde oplossing, hoge capaciteit apparatuur, mag duur zijn.

De uit te wisselen stroom van berichten is massaal, heeft een hoge waarde en vindt plaats tussen een relatief gering aantal deelnemers.
Het hoge gemiddelde bedrag is te verklaren uit de belangrijke transacties voortvloeiend uit het SWIFT-systeem en het Telegirosysteem (men zie hiervoor het laatste jaarverslag van de BankGiroCentrale). Gezien de massaliteit dient het authenticatiesysteem gericht te zijn op het identificeren van zendende en ontvangende organisaties en niet op de daarin werkende functionarissen.
De Stuurgroep voor het Nationaal Betalings Circuit streeft naar een uniforme oplossing voor de

beveiliging van dit berichtenverkeer, waarbij overigens de efficiency niet uit het oog wordt verloren. De besluitvorming hierover is nog niet afgerond.

De output-trajecten: berichtgeving aan cliënt

Dit onderdeel is het laatst geautomatiseerd en geniet wat beveiliging betreft slechts een stiefmoederlijke belangstelling. In feite gaat het hier om de berichtgeving aan cliënten, die tegelijk een verantwoording is van de verrichte handelingen naar aanleiding van de verstrekte opdrachten. Kans op fraude op dit traject lijkt nauwelijks te bestaan. Wellicht is er bij grote ondernemingen op het gebied van electronic banking behoefte aan deze faciliteit.
Hierin bestaat echter geen eenduidig inzicht.

Mogelijkheden voor standaardisatie

Samenvattend kan worden vastgesteld dat de beveiliging van het geautomatiseerde betalingsverkeer gericht is op beveiliging van de overdracht van de gegevens en dat deze verschillend is voor:
- elektronische transacties aangeleverd door particulieren;
- elektronische transacties aangeleverd door bedrijven en instellingen, alsmede electronic banking;
- uitwisseling van financiële berichten tussen de banken; en
- output-verstrekking aan de cliënten.

Regelmatig komt de vraag naar voren: "In hoeverre kunnen wij standaardiseren? Zijn er geen internationale normen die overal toegepast kunnen worden?"

Het antwoord is ja.

Het is mogelijk dat alle banken voor bepaalde trajecten dezelfde methoden en hulpmiddelen toepassen, met andere woorden voor:
a. de aanlevering van opdrachten door de particuliere cliënten;
b. de aanlevering van opdrachten door de zakelijke cliënten;
c. de onderlinge uitwisseling van berichten tussen banken.
Er ontstaan dan vanuit de markt gezien drie gestandaardiseerde systemen.

Er is echter meer. Het is mogelijk bepaalde componenten van de verschillende systemen te uniformeren. Dit geldt voor:
- het gebruik van cryptografische sleutelsystemen;
- het gebruik van algoritmen;
- methoden van sleutelbeheer (key management).

Op dit gebied bestaan er internationale standaards. Gebruikt men dezelfde componenten op de verschillende trajecten, dan is er sprake van een gestandaardiseerde beveiligingsarchitectuur.

Een probleem bij het streven naar standaards is dat de mens achter de techniek aanholt: wij kunnen de ontwikkelingen nauwelijks bijhouden. Het afspreken van standaards kost veel overleg en veel tijd. Vandaar dat er in vele gevallen niet zo maar een standaard voor een bepaalde vorm van beveiliging is te vinden.

Er is echter internationaal een ontwikkeling gaande om te zoeken naar oplossingen. Voor de particuliere opdrachten is reeds een keuze gemaakt.
Voor de aanlevering van zakelijke opdrachten en onderlinge uitwisseling tussen banken zijn de verschillende partijen nog zoekende. Er moet dus nog een weg worden afgelegd om te komen tot een haalbare methode en technieken. Daarna kan worden begonnen met de implementatie.
Een en ander zal een aantal jaren in beslag nemen. Maar de trein is in beweging en zal zeker aankomen.

GEAUTOMATISEERD UITGAAND GELDVERKEER EN HET FRAUDERISICO

door drs. H.C. Kocks RA

Inleiding

Het uitgaand geldverkeer heeft altijd de bijzondere belangstelling genoten van de controlerend accountant. Door de invloed van de automatisering is die belangstelling alleen maar toegenomen. Dit als gevolg van het verschuiven en wegvallen van (direct) waarneembare (controle-)activiteiten en het verdwijnen van tastbare bescheiden in het betaaltraject waardoor het fraudegevaar is toegenomen.

In dit artikel wordt de interne en externe controleproblematiek met betrekking tot het uitgaand geldverkeer in een geautomatiseerde omgeving nader uiteengezet. Uitgaande van de doelstelling van een organisatie rondom het uitgaand geldverkeer worden vervolgens de te onderscheiden schakels in het traject beschreven. Daarna wordt expliciet op de invloed van de automatisering ingegaan. Ten slotte zal een en ander worden geplaatst in het kader van de accountantscontrole.

Het uitgaand geldverkeer

Op velerlei manieren kan uitgaand geldverkeer zich geautomatiseerd manifesteren. Hiertoe worden gerekend lonen, salarissen inclusief provisies en betalingen voortvloeiend uit secundaire arbeidsvoorwaarden, handels- en overige crediteuren alsmede betalingen aan debiteuren (omzetprovisie/bonussen).

Dit artikel richt zich op betalingen aan crediteuren. Van de lezer(es) wordt verwacht dat hij/zij de relatie kan leggen met het andere uitgaande geldverkeer.

Doelstelling

Als doelstelling van een (goede) betalingsorganisatie wordt gezien dat die organisatie en het daarin opgenomen stelsel van interne controlemaatregelen kan waarborgen dat het juiste bedrag aan een rechthebbende wordt uitgekeerd en dat de betaling door één of meerdere daartoe bevoegde functionarissen is geautoriseerd (procuratie). Als een organisatie zodanig van opzet is en als zodanig werkt, is er sprake van een beperkt fraudegevaar.

Het traject I

Als betalingsorganisatie wordt beschouwd het traject vanaf het ontstaan van de verplichting tot het tenietgaan ervan. Op het ontstaan van de verplichting zelf wordt in het kader van dit artikel niet ingegaan. Het te behandelen traject begint na het ontstaan van de verplichting en loopt door tot het tenietgaan ervan. Dit traject (verder schakels genoemd) is te beschouwen als een keten en bestaat uit de volgende schakels:

Schakel 1 (S-1)	Beheersing van het verplichtingenbestand
Schakel 2 (S-2)	Betaalbaarstelling/betalingsvoorstel
Schakel 3 (S-3)	Aanpassing betalingsvoorstel
Schakel 4 (S-4)	Aanmaak betaalmedium
Schakel 5 (S-5)	Routing/Controle/Procuratie
Schakel 6 (S-6)	Afwerking

Schakel 1: Beheersing van het verplichtingenbestand (S-1)

De organisatie dient zodanige controlemaatregelen te bevatten dat ze de blijvende juistheid van het verplichtingenbestand kan waarborgen.

In een geautomatiseerde omgeving worden aangegane verplichtingen met behulp van programmatuur geregistreerd in een geautomatiseerd bestand. In dit bestand worden naast de verplichtingen (de juiste bedragen) zogenaamde vaste gegevens opgenomen om te kunnen waarborgen dat de verplichting wordt geregistreerd ten name van rechthebbende (NAW-gegevens) en dat de betaling te zijner tijd aan rechthebbende geschiedt (bank- c.q. gironummer(s)). Voor het verdere traject is het uit controle-oogpunt van belang dat de organisatie voldoende zekerheden biedt dat dit bestand de juiste vaste en variabele gegevens bevat en blijft bevatten. Uiteindelijk is dit bestand de basis voor het produceren van het betaalmedium (tape/diskette) waarmee opdracht tot betaling aan de bank plaatsvindt.

Of de organisatie voldoende waarborgen biedt is afhankelijk van:
- de aanwezigheid van functiescheiding, i.c. scheiding van beheer, verwerking en controle tussen vaste en variabele gegevens;
- de beschikbaar gestelde (controle)informatie door het geautomatiseerde systeem; hierbij valt te denken aan overzichten met standen c.q. mutaties;
- de aanwezigheid van procedures, waarbij de juiste controles worden verricht met behulp van de juiste controle-informatie.

Schakel 2: Betaalbaarstelling/betalingsvoorstel (S-2)

De organisatie dient waarborgen te bieden dat de juiste en geautoriseerde bedragen betaalbaar worden gesteld aan rechthebbende(n).

Op enig moment zal betaalbaarstelling moeten plaatsvinden. Dit kan op de volgende manieren:
1. Direct bij het invoeren van een mutatie kan een indicatie "betaalbaarstellen" worden meegegeven. Dit wordt dan geëffectueerd door het zetten van een "vlag" of door opname van bijvoorbeeld de datum van betaalbaarstelling. Het zetten van een vlag of het opnemen van een datum is een programmafunctie.
   In geval van on-line-verwerking komt het voor dat de betaalbaarstelling voor wat betreft de hoogte van bedragen gekoppeld is aan toegekende bevoegdheden.
2. Met behulp van speciaal ontwikkelde toepassingsprogrammatuur worden de te betalen posten geselecteerd (bij voorbeeld op datum ouderdom of andere indicatie). Van de geselecteerde posten wordt in het bestand al dan niet een indicatie betaalbaarstelling (vlag) opgenomen. Bij het corrigeren van het betalingsvoorstel dient die vlag weer te verdwijnen.
3. De selectie van de te betalen posten geschiedt met behulp van een utility (standaardhulpprogrammatuur die niet via de systeemontwikkelingsorganisatie wordt ontwikkeld; het is hulpprogrammatuur voor de operator). In het bestand worden geen indicaties met betrekking tot de betaalbaarstelling opgenomen.

Het zichtbaar maken van de betaalbaarstelling kan derhalve door middel van toepassingsprogrammatuur of door middel van een utility. Het resultaat is een **betalingsvoorstel**. Dit betalingsvoorstel dient naast de geselecteerde posten een telling te bevatten van het verplichtingenbestand om vast te kunnen stellen of met het juiste en volledige bestand is gewerkt.

Indien een betalingsvoorstel wordt gemaakt kan dit voorstel als een apart bestand worden vastgelegd al dan niet op een apart medium. Deze mogelijkheid zal zich wellicht alleen voordoen bij de situaties genoemd onder 2. en 3. De verdere verwerking wordt dan verricht met dit aparte bestand. Op de een of andere wijze zal de koppeling met het verplichtingenbestand moeten worden gehandhaafd. Dit kan geautomatiseerd of handmatig plaatsvinden.

Als geen betalingsvoorstel wordt gemaakt zal het te verzenden betaalmedium naar de BGC c.q. Postbank en het daarbij behorend overzicht rechtstreeks worden aangemaakt vanuit het verplichtingenbestand (situatie als onder 1. aangegeven).

Schakel 3: Aanpassing betalingsvoorstel (S-3)

De organisatie dient waarborgen te bieden dat het betalingsvoorstel juist en geautoriseerd wordt aangepast.

Aanpassing van een betalingsvoorstel geschiedt omdat bepaalde posten (nog) niet betaald mogen worden. Correcties op een betalingsvoorstel kunnen zowel in batch-verwerking als on-line worden aangebracht. De praktijk tendeert steeds meer naar on-line-aanpassing. Belangrijk is hierbij **wat** kan worden aangepast.

Uit controle-oogpunt verdient het aanbeveling bij aanpassing van het betalingsvoorstel alleen posten te laten vervallen. Evenals in de vorige schakel geldt dat bij het aanpassen van het betalingsvoorstel de aansluiting met het verplichtingenbestand moet worden gehandhaafd.

Schakel 4: Aanmaak betaalmedium (S-4)

De automatiseringsorganisatie (verwerkingsorganisatie) dient voldoende waarborgen te bieden dat de juiste en geautoriseerde gegevens op het naar de BGC/Postbank te verzenden medium worden opgenomen (juiste bedragen) en het bijbehorend overzicht (voor controledoeleinden).

Het betaalmedium (tape/diskette) met een bijbehorend overzicht wordt door de verwerkingsorganisatie aangemaakt op grond van een (doorlopende) opdracht vanuit de gebruikersorganisatie. De verwerkingsorganisatie dient te waarborgen dat op het betaalmedium dezelfde gegevens worden opgenomen als op het overzicht.

Er wordt wel aangenomen dat het betaalmedium en het overzicht gelijk moeten zijn omdat ze vanuit één bestand worden aangemaakt. Dit hoeft niet het geval te zijn. Beseft dient te worden dat ze meestal gescheiden tot stand komen.

Het overzicht zal meestal tot stand komen via een tussenslag (**spooling** genoemd) vanwege het verschil in de snelheid van verwerking door de CPU en het printproces. Er wordt alvorens er wordt geprint een **spool**-bestand opgebouwd. Van belang is in een dergelijke situatie, in hoeverre zo'n tussenbestand beveiligd is tegen ongeautoriseerde wijziging. Het direct aanbrengen van wijzigingen in data op een **spoolfile** is mogelijk met behulp van hulpprogrammatuur (utilities).

De aanmaak van het betaalmedium kan geschieden door middel van applicatieprogrammatuur (door de gebruiker geautoriseerd) of een utility rechtstreeks vanuit het verplichtingenbestand of vanuit een apart betaalbestand.

Voor de verdere procesgang is het in bepaalde situaties uit controle-overwegingen belangrijk dat minimaal twee betaalmedia worden aangemaakt en na aanmaak samen met het bijbehorend overzicht buiten de verwerkingsorganisatie worden gebracht. Het tweede betaalmedium kan een belangrijke rol spelen indien het eerste medium niet door de BGC/Postbank kan worden verwerkt.

Schakel 5: Routing/Controle/Procuratie (S-5)

De organisatie dient waarborgen te bieden dat een juiste en geautoriseerde betaal-opdracht (= tape/diskette voorzien van een getekend geleidebiljet) met de juiste inhoud wordt verzonden.

Na aanmaak in de verwerkingsorganisatie zullen de betaalmedia met het bijbehorend overzicht die organisatie dienen te verlaten. Deze gaan bijvoorbeeld naar de administratie c.q. interne controle-

afdeling of rechtstreeks naar de procuratiehouder. Vervolgens zullen de stukken (onder andere geleideformulier/betaalopdracht) voor procuratie en verzending in orde worden gebracht.

Afhankelijk van de situatie zal zelfstandig vastgesteld moeten worden of de inhoud van het betaalmedium gelijk is aan het bijbehorend overzicht. Derhalve zijn er situaties denkbaar dat dit mag worden aangenomen. In de praktijk is het zo geregeld dat de verdere controle-activiteiten worden verricht met het bijbehorend overzicht (bij voorbeeld controle van posten op het overzicht met brondocumenten of reeds gecontroleerde informatie). Hierbij wordt dan per definitie aangenomen dat de inhoud van het medium gelijk is aan het bijbehorend overzicht. Het zelfstandig vaststellen - onafhankelijk van de verwerkingsorganisatie - van de overeenkomst tussen het betaalmedium en het overzicht is niet altijd even eenvoudig te realiseren wegens het ontbreken van faciliteiten.

Na controle zal een geleidelijst (betaalopdracht) moeten worden voorzien van de nodige financiële informatie en handtekeningen. Vervolgens vindt verzending van het betaalmedium plaats voorzien van de geleidelijst. Verzending kan rechtstreeks door de procuratiehouder gebeuren maar ook via een "postkamer". Registratie van ingaande en uitgaande betaalmedia is uit oogpunt van controle noodzakelijk.

Betaalmedia worden verwerkt door de BGC/Postbank. De BGC heeft een brochure uitgegeven waarin is opgenomen aan welke voorwaarden moet worden voldaan. Het is aan te bevelen van de meest recente BGC-informatie uit te gaan. In deze informatie is de **contactpersoon** genoemd die de contacten onderhoudt tussen de **cliënt** en de BGC.

Belangrijk is dat de contactpersoon geen bemoeienis heeft met het verdere betalingstraject. Deze contactpersoon wordt namelijk ingeschakeld als er iets "mis" is. Hierin schuilt een potentieel (fraude)risico.

Daarnaast staat in de BGC-informatie vermeld welke controles door de verwerkende instantie worden uitgevoerd alsmede welke informatie de cliënten (kunnen) ontvangen.

Schakel 6: Afwerking (S-6)

Deze schakel dient vast te stellen of de juiste bedragen aan rechthebbenden zijn betaald en als zodanig in de administratie zijn verantwoord.

De verwerking van het betaalmedium zal door de BGC plaatsvinden. Daarna zal de cliënt zijn betaalmedium retour ontvangen alsmede een dagafschrift al dan niet met bijbehorende - gedetailleerde - informatie. Ontvangst van betaalmedia dient te worden geregistreerd.

Beheersingsconcepten in geval van automatisering

Zowel in theorie als in praktijk wordt beklemtoond dat de gebruiker inhoudelijk verantwoordelijk is en blijft voor zijn/haar gegevens in een geautomatiseerde omgeving. Om deze verantwoordelijkheid te kunnen dragen kan die gebruiker in sterke mate afhankelijk zijn van de geautomatiseerde gegevensverwerking. Met opzet is hier "kan zijn" gebruikt. Het is namelijk in sterke mate van de situatie afhankelijk of de gebruiker in deze kan en mag STeunen OP (STOP-situatie) een betrouwbare geautomatiseerde gegevensverwerking of niet (NON-STOP-situatie). Deze STOP- en NON-STOP-situatie worden de twee beheersingsconcepten genoemd.

In het kader van het geautomatiseerd uitgaand geldverkeer is het uit oogpunt van controle van essentieel belang welk beheersingsconcept - al dan niet terecht - van toepassing is. Op beide concepten wordt nader ingegaan.

Concept STOP

Een STOP-situatie houdt in dat de gebruikersorganisatie ervan mag uitgaan dat de verwerkingsorganisatie (verwerking inclusief transport) **betrouwbaar** is. Betrouwbaar betekent in dit kader dat de verwerkingsorganisatie een zodanig stelsel van interne controlemaatregelen bevat dat:
- verwerking van gegevens alleen plaatsvindt met door de verantwoordelijke gebruikers geautoriseerde programmatuur;
- de integriteit in voldoende mate is gewaarborgd van de:
  . in bewaring gegeven "data", zijnde gegevens en programmatuur;
  . in besturingsprogrammatuur opgenomen toegangsregels (gericht op het autorisatie-aspect);
  . informatie tijdens het geautomatiseerd transport in geval van data- c.q. telecommunicatie.

Dit lijkt redelijk eenvoudig realiseerbaar, doch kan zeer complex zijn. Alvorens er sprake kan zijn van een STOP-situatie moet aan de volgende voorwaarden zijn voldaan.

De verwerkingsorganisatie
Met betrekking tot de verwerkingsorganisatie dienen de volgende functiescheidingen te zijn gerealiseerd en te worden ondersteund door middel van adequate procedures en voorschriften:
- tussen gebruikers- en verwerkingsorganisatie. Het doel hiervan is om te voorkomen dat de gebruikersorganisatie ongeautoriseerd invloed kan hebben op het geautomatiseerd verwerkingsproces. Indien dat wel zo is kan de verwerkingsorganisatie de haar toebedeelde verantwoordelijkheid niet meer dragen;
- tussen de systeemontwikkelings- (inclusief onderhoud) en de verwerkingsorganisatie. Deze functiescheiding heeft als doel te voorkomen dat eenmaal door de gebruiker geaccepteerde en aan de verwerkingsorganisatie overgedragen programmatuur ongeautoriseerd door de systeemontwikkelingsorganisatie kan worden gewijzigd;
- tussen systeemprogrammering en verwerking. Deze functiescheiding is nodig om te voorkomen dat gedefinieerde en aan de verwerkingsorganisatie overgedragen besturingsprogrammatuur (operating system etc.) ongeautoriseerd door systeemprogrammering kan worden gewijzigd. Systeemprogrammering is de functie die de van de leverancier verkregen besturingsprogrammatuur pasklaar maakt c.q. onderhoudt voor de verwerkingsorganisatie;
- binnen de verwerkingsorganisatie tussen operating en bewaring (van gegevens, programmatuur etc.). Het doel hiervan is dat binnen de verwerkingsorganisatie gegevens en/of data niet ongeautoriseerd kunnen worden aangepast. De verwerkingsorganisatie beschikt immers over alle componenten om wijzigingen te kunnen aanbrengen (apparatuur, systemen, toepassingsprogrammatuur en gegevens).

De voornoemde functiescheidingen dienen **tijdens** de geautomatiseerde gegevensverwerking blijvend te worden gehandhaafd. Controle op het verwerkingsproces is derhalve noodzakelijk.

Reeds aangegeven is dat het realiseren van de functiescheidingen een complexe zaak kan zijn. De genoemde functiescheidingen dienen organisatorisch, hardware- en software-matig gerealiseerd te zijn. De belangrijkste is de software-matige, die het minst zichtbaar is en het moeilijkst vast te stellen. Om dit te kunnen is specifieke deskundigheid vereist (EDP-auditing-kennis).

In het kader van de administratieve organisatie en interne controle zijn de termen (on)vervangbaar en (on)misbaar belangrijk. Zeker als het om functiescheiding gaat. In een STOP-situatie zijn voornoemde functiescheidingen onvervangbaar **en** onmisbaar en derhalve noodzakelijk. Indien ze niet zijn gerealiseerd kan er **geen** sprake zijn van een **betrouwbare** verwerkingsorganisatie.

De systeemontwikkelingsorganisatie (inclusief onderhoud)
In een STOP-situatie dient er sprake te zijn van een betrouwbare systeemontwikkelingsorganisatie. Dit houdt in dat deze organisatie zodanige waarborgen biedt dat slechts systemen worden ontwikkeld volgens goedgekeurde gebruikersspecificaties. Anders gezegd, dat systemen worden ontwikkeld die zodanige (controle-)informatie opleveren dat de gebruikersorganisatie - afhankelijk van het beheersingsconcept - zelfstandig de **volledigheid** en juistheid van de verstrekte informatie kan vaststellen ten aanzien van bestanden en mutaties. Bovendien zal er een adequate over-

drachtsprocedure (administratief en fysiek) moeten zijn tussen gebruikersorganisatie/systeemontwikkeling enerzijds en verwerkingsorganisatie anderzijds.

De gebruikersorganisatie
Uitgaande van een betrouwbare verwerkings- en systeemontwikkelingsorganisatie dient de gebruikersorganisatie het volgende aanvullend te doen:
- het op een juiste manier definiëren en controleren van de toegangsregels die in de besturingsprogrammatuur moeten worden opgenomen. Als dit niet geschiedt volgens de "regels" kunnen ongeautoriseerden toegang verkrijgen tot programmatuur en gegevens;
- controle uitvoeren op de volledigheid en juistheid van de **ingevoerde** mutaties. Immers, het mogen accepteren dat met geautoriseerde programmatuur wordt gewerkt houdt niet in dat tevens de opgeleverde informatie volledig en juist is. De verwerking van foutieve invoer met geautoriseerde programmatuur levert foutieve (controle-)informatie op.

Een organisatie is er niet bij gebaat dat op **enig moment** van een STOP-situatie sprake is. Er dient bij voortduring van een STOP-situatie sprake te zijn. Dit houdt in dat een onderzoek gericht op opzet en bestaan (is toetsing van de werking op enig moment) onvoldoende is en dat toetsing van de werking (is voortdurende toetsing van het bestaan) noodzakelijk is.

Concluderend kan worden gesteld dat een STOP-situatie een controleprogramma vereist waarbij bij voortduring de werking van een betrouwbare verwerkings- en systeemontwikkelingsorganisatie wordt getoetst.

De desbetreffende verantwoordelijke functionarissen dienen van de uitkomsten van de toetsingswerkzaamheden op de hoogte te worden gebracht om hun verantwoordelijkheid ten aanzien van volledigheid, juistheid en autorisatie van (controle-)informatie nog te kunnen dragen.

Concept NON-STOP

Indien zich een situatie voordoet waarbij hetgeen onder het concept STOP is weergegeven niet is gerealiseerd, is er sprake van een NON-STOP-situatie. Dit houdt in dat de gebruikersorganisatie er **niet** van mag uitgaan dat:
- alleen met geautoriseerde programmatuur wordt gewerkt;
- de integriteit gewaarborgd wordt van:
  . in bewaring gegeven data;
  . de in besturingsprogrammatuur opgenomen toegangsregels;
  . de informatie tijdens geautomatiseerd transport.

Daarenboven zijn de vereiste functiescheidingen nog wel onvervangbaar maar niet onmisbaar. Dit alles houdt in dat de gebruikersorganisatie **zelfstandig** de (blijvende) volledigheid, juistheid en autorisatie van de geautomatiseerd verstrekte informatie dient vast te stellen ten aanzien van **bestanden** en **mutaties**. De geautomatiseerde gegevensverwerking zal derhalve de daarop gerichte (controle-)informatie dienen op te leveren.

Concept STOP versus NON-STOP

In het voorgaande zijn de beide beheersingsconcepten als uitersten behandeld. Uitersten, omdat daartussen sprake is van een grijs gebied. Dat is ook hier het geval. Een perfecte STOP-situatie zal zich in de praktijk wellicht niet of nauwelijks voordoen. De relevante vraag in dit kader is derhalve in hoeverre bij een niet of minder perfecte STOP-situatie het geautomatiseerd verwerkingsproces zal leiden tot foutieve (controle-)informatie.

De term risico-analyse - met alle problemen van dien - is hier op zijn plaats omdat nog geen (wiskundige) hulpmiddelen voorhanden zijn die antwoord kunnen geven op de vraag in welke mate een "onvolkomen" of "minder betrouwbaar" proces tot onjuiste uitkomsten leidt. Risico-analyse dient in casu te worden aangevuld met "professional judgement". Geen elegante oplossing maar wel de praktijk.

Controlebenadering preventief versus repressief

Naast de behandeling van de beheersingsconcepten is het in dit kader van belang in te gaan op de controlebenadering die in een organisatie - al dan niet bewust - wordt gehanteerd. In de eerste periode van geautomatiseerde gegevensverwerking was het normaal dat (controle-)informatie werd opgeleverd om achteraf vast te kunnen stellen of de gegevens volledig en juist waren verwerkt. Correctieprocedures maakten normaal onderdeel uit van het gegevensverwerkend traject.

Met de komst van on-line-verwerking werden controles meer verlegd naar het voortraject. Door de introductie van password-systemen en geprogrammeerde controles in on-line-programmatuur werd het accent van repressieve controles verschoven naar preventieve. Controle vooraf levert **geautoriseerde** toegang, **schone** invoer en **juiste** verwerking op. Controle achteraf wordt tot een minimum beperkt of blijft geheel achterwege. Dit is de ontwikkeling die zich heeft voltrokken. De vraag is of dit terecht is. Uit de behandeling van de beheersingsconcepten valt af te leiden dat een preventieve controlebenadering slechts mag worden gehanteerd in geval van een STOP-situatie. Ook hier is geen sprake van een zwart-wit-situatie. Er kunnen ook situaties ontstaan waarbij er van een goed evenwicht tussen preventieve en repressieve controlemaatregelen sprake is (mix).

Relatie beheersingsconcept en controlebenadering

Het zal duidelijk zijn dat het beheersingsconcept op de een of andere wijze onlosmakelijk is verbonden aan de controlebenadering. Uit de praktijk blijkt dat niet doelbewust voor een concept en/of benadering wordt/is gekozen. Daardoor wijkt de **werkelijke** situatie dan ook af van die waarvan het management en de organisatie uitgaat met alle mogelijke gevolgen van dien. Met andere woorden: aangenomen wordt dat van een STOP-situatie met controlebenadering "preventief" sprake is terwijl dit in het geheel niet realiseerbaar is. Gegeven de twee beheersingsconcepten en de drie controlebenaderingen geeft dit zes mogelijke situaties die in figuur 1 zijn weergegeven en waarop hierna kort wordt ingegaan.

De indruk zou kunnen worden gewekt dat in een STOP-situatie elke controlebenadering zodanig zou kunnen worden gehanteerd dat van een sluitend stelsel van controlemaatregelen zou kunnen worden gesproken. De gedachte zou kunnen postvatten dat in een STOP-situatie de controlebenadering wordt bepaald door het efficiency-aspect.

Dit is echter niet het geval en daarmee wordt de kern geraakt van het geautomatiseerd uitgaand geldverkeer. De controlebenadering wordt i.c. bepaald door de mogelijkheid of een verrichte betaling, die om welke reden dan ook foutief blijkt te zijn, **tijdig** achteraf kan worden gecorrigeerd. Indien deze mogelijkheid is uitgesloten zal de preventieve controlebenadering de meest aangewezen zijn. Indien in een dergelijke situatie **bewust** voor een repressieve benadering wordt gekozen of voor een mix, wordt **bewust** risico genomen. De klemtoon is gelegd op bewust. De praktijk leert dat het bewust kiezen voor een benadering niet veel voorkomt, mede gezien het feit dat dit evenmin voor een STOP-situatie het geval is.

Een nadere beschouwing van de NON-STOP-situatie leert dan, dat in dit geval slechts van een repressieve controlebenadering sprake mag zijn. Een preventieve benadering is uitgesloten omdat niet van de blijvende juistheid van toegangsregels en toepassingsprogrammatuur mag worden uitgegaan. Zelfstandige vaststelling van de volledigheid, juistheid en geautoriseerdheid van de verstrekte (controle-)informatie door de gebruiker is noodzakelijk.

Beheersings-concept / Controle-benadering	STOP	NON-STOP
Preventief		
Repressief		
Mix preventief/ repressief		

Figuur 1. Combinaties van beheersingsconcepten en controlebenaderingen.

Een NON-STOP-situatie gecombineerd met een mix van preventieve en repressieve controle-maatregelen zal niet getuigen van doelmatigheid. Achteraf zal vastgesteld moeten worden of de preventieve controlemaatregelen hebben gewerkt. Er mag niet zonder die vaststelling achteraf worden aangenomen dat ze hebben gewerkt.

Gerelateerd aan de huidige praktijk, kan niet worden ontkend dat de nadruk steeds meer is komen te liggen op een preventieve controlebenadering. On-line-verwerking is niet meer weg te denken. De gebruikersorganisatie gaat ervan uit - op grond van onvoldoende zichtbare (controle-)informatie - dat vertrouwd mag worden op een betrouwbare verwerkingsorganisatie. De noodzakelijke controlehandelingen achteraf verdwijnen steeds meer.

Mede gezien het feit **wanneer** van een betrouwbare geautomatiseerde verwerking gesproken mag worden is het evident dat in vele gevallen **onbewust** risico wordt gelopen. Een en ander geplaatst in het kader van het uitgaand geautomatiseerd geldverkeer is het onmiskenbaar dat onbewust risico wordt gelopen als er geen sprake is van een duidelijk beheersingsconcept met een bijbehorende controlebenadering. Indien die duidelijkheid niet wordt geschapen zal dat risico in de toekomst groter worden. De ontwikkelingen op automatiseringsgebied (data-/telecommunicatie) gaan namelijk in de richting dat een STOP-situatie met controlebenadering "preventief" voorwaarde is om aan de doelstelling van het uitgaand geldverkeer te blijven voldoen en het frauderisico te beperken tot een aanvaardbaar niveau.

Het traject II

Na de eerste beschrijving van het traject is het van wezenlijk belang het traject nogmaals de revue te laten passeren. Ingegaan wordt op de relevante (controle)maatregelen per schakel in relatie tot het geldende beheersingsconcept.

Concept STOP

Uitgaande van een **betrouwbare** verwerking (zie het hoofdstuk beheersconcepten in geval van automatisering) mag de gebruiker zich ten aanzien van de inhoudelijke gegevens in S-1 beperken tot controle op de volledigheid en juistheid van de invoer gesplitst naar vaste (bank- c.q. gironummers) en variabele gegevens. De volledigheid en juistheid kan worden gecontroleerd mits de gebruiker de juiste informatie ontvangt die gedefinieerd is bij de ontwikkeling van systemen. De controle op

juistheid van invoer kan integraal of via een deelwaarneming plaatsvinden, vanuit geautomatiseerd verkregen informatie met brongegevens.

De **controle op de juiste invoer** kan nog op een andere wijze geschieden. Door middel van een steekproef op het bestand waarin de invoer is verwerkt.

Gesteld is dat een optimale STOP-situatie nagenoeg niet voorkomt in de praktijk waardoor foutieve geautomatiseerde verwerking tot de mogelijkheden behoort. Het is in voorkomende situaties aan te bevelen een wiskundige steekproef uit te voeren op het bestand (i.c. verplichtingenbestand) waarin de invoer - al dan niet getransformeerd door toepassingsprogrammatuur - is opgenomen. Door nu zowel de juistheid van de geselecteerde posten als de juistheid van de daarbij behorende invoer vast te stellen kan min of meer een oordeel worden verkregen over de mate van juistheid van in het bestand opgenomen posten. Indien onjuiste posten in een bestand zijn opgenomen kan worden vastgesteld of die onjuistheid door **invoer** of **verwerking** is veroorzaakt. Hierdoor is een extra "check" op de verwerking verkregen. Gesteld zou kunnen worden dat bij een dergelijke controle een STOP-situatie niet nodig zou zijn omdat de controle uitkomst-gericht is. Dit is niet geheel waar. Bij het beperken van de omvang van de steekproef dient er uit efficiency-oogpunt met de kwaliteit van de verwerkings- en gebruikersorganisatie rekening te worden gehouden.

Een dergelijke controle is vooral aan te bevelen in situaties waar sprake is van **massaliteit in invoer.** Integrale controle wordt niet meer mogelijk geacht waarbij overgegaan wordt tot (ongestructureerde) deelwaarneming met alle gevolgen van dien. Door de voorgestelde controle, indien goed uitgevoerd, kan op efficiënte wijze risicobeperking plaatsvinden.

Bij de betaalbaarstelling (S-2) van verplichtingen zal de gebruiker zich eveneens vooral op de invoercontrole dienen te richten. Uit de eerdere beschrijving van deze schakel bleek dat er over het algemeen op drie manieren betaalbaarstelling plaatsvindt, te weten:

1. direct bij het invoeren van de mutatie in het bestand. In dit geval valt de controle op de betaalbaarstelling onder de invoercontrole van het verplichtingenbestand;
2. met behulp van speciaal ontwikkelde toepassingsprogrammatuur. Deze programmatuur mag als betrouwbaar worden geaccepteerd. Alleen controle op de variabele betaalbaarstellingscriteria dient nog te worden uitgevoerd. Informatie dient derhalve beschikbaar te komen;
3. selectie van te betalen posten wordt verricht met behulp van hulpprogrammatuur (utilities). Aangezien van een betrouwbare verwerkingsorganisatie mag worden uitgegaan zal met de juiste utilities worden gewerkt. De controle kan beperkt blijven tot de variabele selectiecriteria. De gebruiker dient ook hierover controle-informatie te ontvangen.

Indien aanpassing van het betalingsvoorstel (S-3) plaatsvindt, zal de gebruikersorganisatie zich kunnen beperken tot de controle op de aangebrachte wijzigingen. Zoals eerder reeds is aangegeven, is het raadzaam geen inhoudelijke wijzigingen toe te staan maar alleen een betaalbaarstelling te laten vervallen.

De praktijk wijst uit dat het aanbrengen van mutaties in het verplichtingenbestand alsmede de betaalbaarstelling en het eventueel aanpassen daarvan steeds meer on-line plaatsvindt. In een dergelijke situatie dient de gebruikersorganisatie de bevoegdheden juist te hebben toegekend en aangebracht in toegangscontroletabellen, zijnde bestanden. Dit houdt in dat mutaties in bestanden worden aangebracht waarop derhalve invoercontrole noodzakelijk is. De gebruiker zal in zo'n situatie controle-informatie moeten ontvangen. Een betrouwbare verwerkingsorganisatie zorgt in een STOP-situatie voor de integriteit van de toegangscontroletabellen.

Naast het feit dat bevoegdheden worden opgenomen in speciale **besturings**programmatuur komt het nog steeds voor dat toegangsbevoegdheden in **toepassings**programmatuur is opgenomen. In een dergelijke situatie is het controleren van de juiste toegangsregels onderdeel geworden van de test- en acceptatieprocedure tijdens de systeemontwikkeling. Bij het wijzigen van toepassingsprogrammatuur zal derhalve tevens aandacht aan de toegangsregels moeten worden gegeven. Omgekeerd houdt het wijzigen van toegangsregels, het wijzigen van toepassingsprogrammatuur in. (Dit is meestal het geval als sprake is van menu-hiërarchie: menu-gestuurde programmatuur.)

Verder is reeds aangegeven dat de betaalbaarstelling direct kan plaatsvinden in het verplichtingenbestand maar dat ook een separaat bestand kan worden aangemaakt waarmee de verdere verwerking plaatsvindt. Aangegeven is daarbij dat in het laatste geval het aparte bestand blijvend dient te sluiten met het verplichtingenbestand. Die blijvende sluiting kan geautomatiseerd of handmatig worden geëffectueerd. Geautomatiseerd houdt in dat bij de ontwikkeling van de toepassingsprogrammatuur daaraan aandacht is besteed. Extra controle is in een STOP-situatie dan niet nodig. Indien de blijvende relatie met het verplichtingenbestand handmatig moet worden vastgesteld zullen mutaties gecontroleerd moeten worden; zowel de blijvende sluiting als de juistheid van de mutatie (invoer) in beide bestanden.

Het aanmaken van het betaalmedium en het bijbehorende overzicht (S-4) geschiedt door de verwerkingsorganisatie. Deze is betrouwbaar en derhalve mag worden aangenomen dat dit op de juiste wijze geschiedt. Het gescheiden aanmaken van betaalmedium en het bijbehorend overzicht is niet meer relevant. Evenmin hoeft de gebruiker aandacht te besteden aan de bewaring van de betaalmedia. Ingeval er tegelijk twee worden aangemaakt mag het tweede medium door de verwerkingsorganisatie worden bewaard. Zelfs kan worden besloten slechts één betaaltape of -diskette te laten aanmaken. Indien een tweede nodig is wordt een juiste aangemaakt.

Door het voorgaande komt S-5 (Routing/Controle/Procuratie) in een apart daglicht te staan. Het betaalmedium met bijbehorend overzicht gaat naar de desbetreffende instantie(s) voor verdere verwerking. Verwerking houdt in dat:
- geen controle meer hoeft plaats te vinden op het feit of het betaalmedium dezelfde inhoud heeft als het bijbehorend overzicht. Het overzicht mag verder als controlemiddel worden gebruikt;
- geen controle van betaalbaar gestelde verplichtingen met brondocumenten meer hoeft plaats te vinden. Door afdoende controles in het voortraject is dit in feite niet meer nodig.

In een STOP-situatie kan de procuratiehouder zich beperken tot het kritisch doornemen van het overzicht van betaalbaar gestelde verplichtingen en de daarbij behorende betaalopdracht ondertekenen. De verdere behandeling van zowel het betaalmedium als de betaalopdracht zal volgens de voorschriften dienen te geschieden. Dit levert uit controle-oogpunt geen specifieke punten op.

De afwerking (S-6) zal zich in een STOP-situatie beperken tot het afhandelen van het betaalmedium dat retour is ontvangen van de BGC of de Postbank alsmede de afmutatie van de bank. Detailcontrole op door de bank verwerkte betalingen is in de praktijk veelal niet meer mogelijk omdat geen gedetailleerde informatie meer wordt verstrekt. In een STOP-situatie is dit begrijpelijk. De controlebenadering is meestal preventief waardoor gedetailleerde controle achteraf niet meer nodig wordt geacht. Het is derhalve een kwestie van risico-afweging. Hiertegen bestaat geen bezwaar mits het maar doelbewust gebeurt.

Concept NON-STOP

Kortweg gesteld is het in een NON-STOP-situatie noodzakelijk dat de gebruikersorganisatie **zelfstandig** naast de volledigheid en juistheid van de **geautomatiseerd** verwerkte en verstrekte informatie ook de geautoriseerdheid ervan vaststelt. Alle on-line-verwerkingen met password-systemen in de schakels 1 t/m 3 ten spijt.

Wat houdt dit uit controle-oogpunt nu in. Dit houdt in dat alvorens het betaalmedium met een getekende betaalopdracht naar de BGC/Postbank wordt verzonden **vooraf**:
- wordt vastgesteld dat de inhoud van het betaalmedium gelijk is aan het bijbehorend overzicht dat voor verdere controle- en verwerkingsdoeleinden wordt gebruikt;
- controle plaatsvindt van het bijbehorend overzicht:
  . met brondocumenten (goedgekeurde facturen op juistheid bedrag en bank- c.q. gironummer rechthebbende);
  . met de juiste gecontroleerde informatie uit de schakels 1 t/m 3.

Hiermee wordt aangegeven dat de meest belangrijke schakel in het traject bij een NON-STOP-situatie schakel 5 is.

Uit interne controle-oogpunt is het derhalve essentieel deze schakel zo sterk mogelijk te maken. Is dat op de een of andere wijze niet mogelijk dan kan het frauderisico worden beperkt tot de verwerkingsorganisatie (S-4) mits de controles in de schakels 1 t/m 3 voldoende gericht zijn op het zelfstandig door de gebruikersorganisatie vaststellen van de volledigheid, juistheid en geautoriseerdheid van de geautomatiseerd verwerkte en verstrekte informatie. Als de controles in dit deel van het traject als zwak of onvoldoende zijn aan te merken kan dat een versterkende invloed hebben op het frauderisico.

Een aantal keren is **zelfstandige** vaststelling van de overeenstemming tussen de inhoud van het betaalmedium en het bijbehorend overzicht genoemd. Dit is (nog) niet eenvoudig te realiseren. De meeste procuratiehouders of controlefunctionarissen beschikken (nog) niet over een **tape-unit.** Met opzet is "nog" tussen haakjes geplaatst. Voor personal computers (PC's) bestaan thans wel tape-units. Dit vergt echter een investering. Deze investering dient te worden afgewogen tegen het feit hoe hoog het frauderisico wordt ingeschat, derhalve een kosten-nutvraagstuk. Er wordt op gewezen, dat in het merendeel van de gevallen deze afweging niet plaatsvindt omdat onvoldoende de **betrouwbaarheid** van het gehele betaaltraject duidelijk is.

Bij gebruik van diskettes is het eenvoudiger zelfstandig **vooraf** te bepalen of de inhoud van de diskette gelijk is aan het bijbehorend overzicht. In een PC-omgeving waar gebruik wordt gemaakt van tapes en diskettes is tevens de mogelijkheid aanwezig dat de inhoud ervan dan ongeautoriseerd wordt aangepast. Een beschermde omgeving zonder programmatuur om te wijzigen is derhalve noodzakelijk. Gesteld wordt wel eens dat de procuratiehouder de zwakke plek in het geheel is. Wijzigingen kunnen dan door hem/haar worden aangebracht. Dit valt niet te ontkennen maar dit is geen automatiseringsvraagstuk. De procuratiehouder heeft per definitie de bevoegdheid om betaalopdrachten te verstrekken.

In de praktijk komt het voor dat deze tape ter controle op de juiste inhoud aan de verwerkingsorganisatie wordt aangeboden om de inhoud ervan separaat te laten afdrukken. Hierbij dient te worden gerealiseerd welke waarde eraan moet worden toegekend. Er is immers sprake van een NON-STOP-situatie.

Het frauderisico

In dit kader maakt het veel uit van welk beheersingsconcept sprake is. Bij een STOP-concept zal het gehele betalingstraject moeten worden onderzocht om de hoogte - alsmede de ernst - van het frauderisico te kunnen bepalen. Immers, de kwaliteit, noodzaak en omvang van de gebruikerscontroles worden in zeer belangrijke mate bepaald door de kwaliteit van de automatisering, zijnde de verwerkings- en ontwikkelingsorganisatie. Dit is in dubbel opzicht niet eenvoudig. Zowel het bepalen van het frauderisico enerzijds als de advisering om het frauderisico te beperken anderzijds, vereist grote deskundigheid op het gebied van automatisering en controle.

Eenvoudiger is het NON-STOP-concept. Als schakel 5 **dicht** zit is het frauderisico nihil. Indien dat niet het geval is zal advisering zijn gericht op het versterken van die schakel. Blijkt dit niet mogelijk te zijn dan gaat van alle voorgaande schakels in principe een versterkende invloed uit. Blijkt uit nader onderzoek dat van de schakels 1 t/m 3 geen versterkende invloed uitgaat dan blijft de invloed van S-4 over. Deze is dan niet te beperken aangezien van een NON-STOP-concept sprake is waarbij - om welke reden dan ook - S-5 onvoldoende mogelijkheid tot controle biedt.

Datacommunicatie

Datacommunicatie neemt hand over hand toe. Hiermee wordt het transport van informatie geautomatiseerd. Aan de verwerkingsorganisatie wordt de geautomatiseerde transportfunctie toegevoegd. Zij dient er derhalve voor te zorgen dat de implementatie van de datacommunicatiefaciliteiten met de bijbehorende besturingsprogrammatuur (toegangsregels) zodanig geschiedt dat de integriteit van de informatie tijdens het transport kan worden gewaarborgd.

Hierbij is een kanttekening op zijn plaats. Die waarborging van de integriteit kan alleen worden afgegeven voor het transporterende traject dat binnen de eigen verantwoordelijkheid van de verwerkingsorganisatie valt. Ten aanzien van openbare netwerken kan deze zekerheid niet worden gegeven.

De verwachting is dat in de (nabije) toekomst het geautomatiseerd uitgaand geldverkeer meer via datacommunicatie zal plaatsvinden. De vraag is derhalve wat de invloed ervan zal zijn op hetgeen tot nu toe besproken is. De in dit artikel gehanteerde doelstelling blijft onverkort van kracht. De realisatie ondergaat wijziging. De belangrijkste wijzigingen zijn:

- door de toenemende integratietendensen en on-line-verwerking zullen de (controle)handelingen met betrekking tot de betaalbaarstelling zich gaan concentreren op het verplichtingenbestand. De nadruk komt hierbij dan te liggen op de ontwikkeling van betrouwbare programmatuur alsmede het definiëren en controleren van de juiste toegangsregels die in de besturings- of toepassingsprogrammatuur moet worden opgenomen;
- het aanmaken van het betaalmedium met bijbehorend overzicht alsmede het geleidebiljet (betaalopdracht) vervalt. Bij de bank vervalt hiermee de mogelijkheid tot het vergelijken van handtekeningen;
- de procuratiefunctie is geautomatiseerd. Deze functie is nu opgenomen in de besturings- (toegangscontroletabellen) of toepassingsprogrammatuur met alle fraudemogelijkheden van dien.

Het zal duidelijk zijn dat de gebruiker nog meer (zo niet geheel) afhankelijk wordt van de automatisering en er in feite sprake dient te zijn van een STOP-concept om het frauderisico onder een aanvaardbaar niveau te houden. Het is derhalve aan te bevelen de kwetsbaarheid te onderzoeken alvorens tot een dergelijke betaalwijze over te gaan. Het is verleidelijk van geboden technische mogelijkheden gebruik te (moeten) maken. Om een ongewenste situatie te vermijden is het verstandig vooraf de mogelijke risico's in te schatten. Ook hier geldt het spreekwoord:

"Bezint eer ge begint."

Over het algemeen kan worden gesteld dat in geval van datacommunicatie het beheersingsconcept STOP van toepassing dient te zijn met als bijbehorende controlebenadering "preventief".

Accountantscontrole

Bij nagenoeg elke jaarrekeningcontrole wordt de accountant thans op enigerlei wijze geconfronteerd met geautomatiseerd uitgaand geldverkeer. Dit geldverkeer heeft, zoals in de inleiding gesteld, altijd de bijzondere aandacht gehad van de accountant. Deze zal uit hoofde van zijn functie als controleur van de jaarrekening binnen gestelde toleranties moeten vaststellen of uitgaven juist (en geautoriseerd) hebben plaatsgevonden aan rechthebbenden. Om dit te kunnen vaststellen staan de accountant twee controlebenaderingen ter beschikking die als gegevensgericht (substantive) en systeemgericht (reliance) in de literatuur omschreven staan. Beide zullen in dit kader nader worden toegelicht.

Gegevensgericht

Bij deze benadering gaat de accountant na of in de **gebruikersorganisatie** de **onvervangbare** en **onmisbare** functiescheidingen zijn gerealiseerd en door adequate controleprocedures worden ondersteund. Dit is de zogenaamde minimumpositie. Vervolgens richt de accountant zich op het cijfermateriaal (uitgaande verrichte betalingen) en stelt daarvan **achteraf** vast of deze juist zijn verricht aan rechthebbenden. Deze controle wordt meestal verricht door middel van deelwaarneming. De omvang van de deelwaarneming wordt door de kwaliteit van de gebruikersorganisatie bepaald. Automatisering speelt hierbij **geen** rol. Als de accountant fraude constateert is dit achteraf. Is de fraude juist verwerkt in de jaarrekening dan treft de accountant geen blaam. Hij zal vervolgens de oorzaak van de fraude bepalen en dienaangaande adviseren. Zijn advies zal zich richten op de gebruikersorganisatie.

Systeemgericht

Bij deze benadering maakt de accountant meer gebruik van de aanwezige controlemaatregelen dan bij de gegevensgerichte controlebenadering. De omvang van de controles op het cijfermateriaal zullen derhalve beperkter zijn dan bij de gegevensgerichte benadering. Als gesproken wordt over **aanwezige controlemaatregelen** dan is het noodzakelijk het volgende onderscheid te maken:

1. de accountant maakt gebruik van de aanwezige controlemaatregelen **inclusief** die in de verwerkings- en systeemontwikkelingsorganisatie (systeemgerichte controle **met** automatisering). Deze controlebenadering is slechts mogelijk indien het beheersingsconcept STOP van toepassing is. In het voorgaande is aangegeven aan welke vereisten een organisatie moet voldoen;
2. de accountant maakt gebruik van de aanwezige controlemaatregelen **exclusief** die in de verwerkings- en systeemontwikkelingsorganisatie (systeemgerichte controle **zonder** automatisering). De controlebenadering is zowel mogelijk in een STOP- als NON-STOP-situatie.

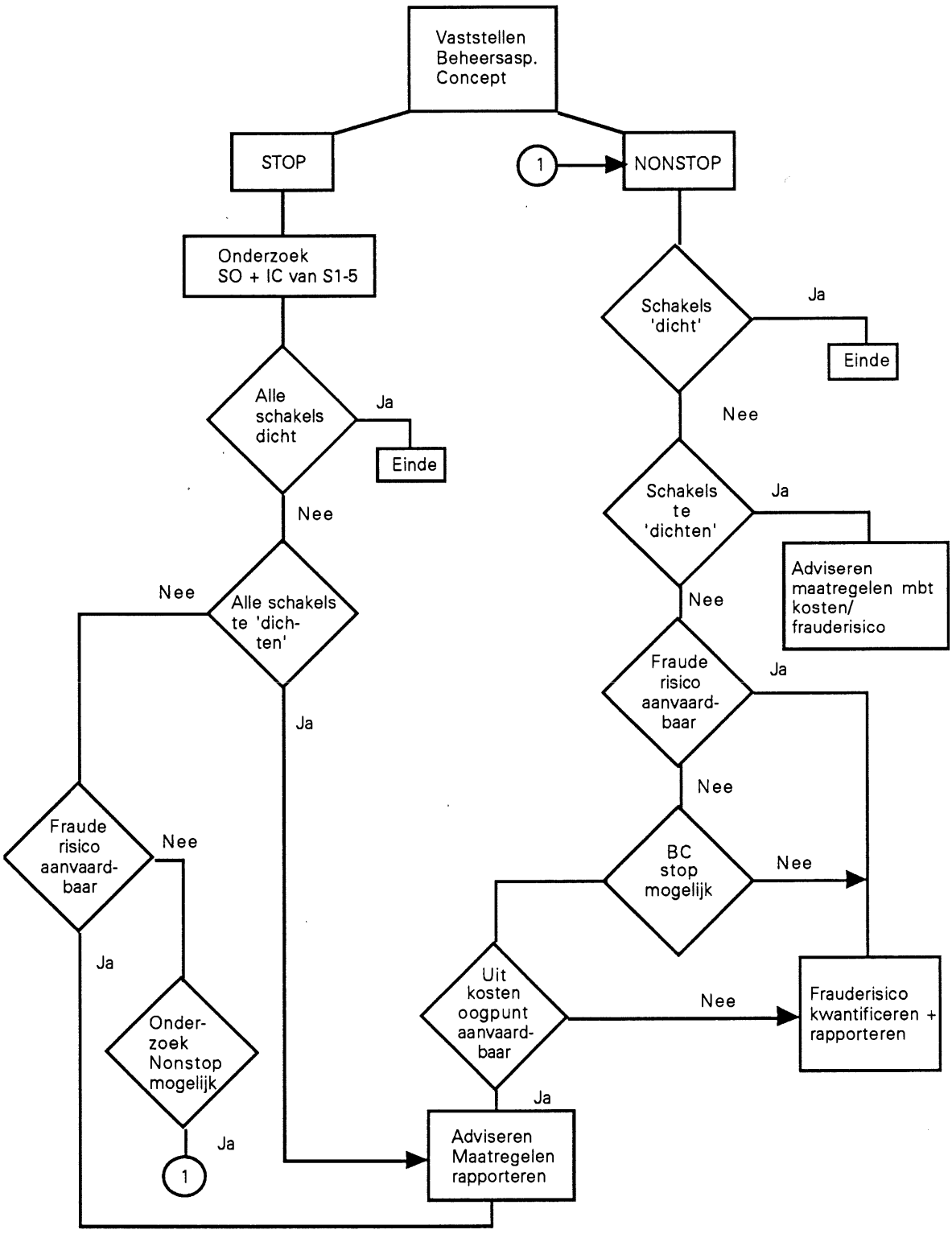
Zowel bij een systeemgerichte als gegevensgerichte benadering zal een fraude worden ontdekt als de accountant een volkomen onderzoek verricht. Dit is echter achteraf. De beide systeemgerichte controlebenaderingen geven de accountant meer mogelijkheden te adviseren waardoor fraude kan worden voorkomen.

Frauderisico

Naast de jaarrekeningcontrole kan er behoefte bestaan aan een onderzoek naar het mogelijke frauderisico. Dit onderzoek draagt dan een specifiek karakter, ook wel "onderzoek betalingsorganisatie" genoemd. In de in dit artikel genoemde doelstelling is het voorkomen van fraude een belangrijk aspect. Aan te bevelen is het onderzoek als volgt uit te voeren:

- bepaal van welk beheersingsconcept sprake is. De uitkomst hiervan is bepalend voor de verder te verrichten werkzaamheden. Het gaat derhalve om een STOP- of NON-STOP-situatie. Of van een STOP-situatie sprake is kan op eenvoudige wijze worden vastgesteld. Er dient dan een werkprogramma te zijn, gericht op de toetsing van de permanente werking van een betrouwbare verwerkings- (inclusief transport) en ontwikkelingsorganisatie en dat wordt uitgevoerd door een van die organisaties losstaand deskundige. Indien dat ontbreekt is een NON-STOP-situatie van toepassing;
- bij een STOP-situatie, waarbij de accountant zich een oordeel heeft gevormd over het werkprogramma, de uitvoering en de uitkomsten, richt hij/zij zich verder op alle overige schakels van het onderhavige traject. Per schakel moet de organisatie aan de (sub)doelstelling beantwoorden. De sterkte van de totale keten wordt bepaald door de zwakste schakel;
- in geval van een NON-STOP-situatie richt de accountant zich in eerste instantie op de interne controlemaatregelen in schakel 5. Deze schakel kan zodanige controlemaatregelen bevatten dat volledig aan de doelstelling wordt beantwoord. Is de mogelijkheid niet aanwezig dan zal de accountant de interne controle dienen te onderzoeken van **alle** overige schakels. De zwakke schakel in de keten blijft schakel 4 (verwerkingsorganisatie) aangezien er sprake is van een NON-STOP-situatie. De accountant zal zich bij advisering met betrekking tot de te nemen maatregelen in de diverse schakels moeten afvragen wat de effectiviteit ervan zal zijn alsmede de daarmee gepaard gaande kosten.

Het traject in geval van een onderzoek naar fraudemogelijkheden is in figuur 2 opgenomen.



Figuur 2.

Ten slotte

De controleproblematiek bij geautomatiseerd uitgaand geldverkeer is in dit artikel benaderd vanuit de twee beheersingsconcepten STOP en NON-STOP die als uitersten zijn weergegeven. Daartussen is uiteraard een grijs gebied te onderkennen dat de meeste overeenstemming met de praktijk te zien geeft. Het voorgaande dient derhalve als een denkkader beschouwd te worden en samen met bijvoorbeeld de eigen kennis en ervaring gebruikt te worden bij het toetsen van een gegeven situatie. De deskundigheid van betrokkenen zal uitmaken in hoeverre het samenstel van (controle)maatregelen in een gegeven situatie als (on)voldoende wordt aangemerkt. Tevens is die deskundigheid van essentiële betekenis als het om advisering gaat in een geautomatiseerde omgeving. Het datacommunicatietijdperk is ingetreden. Deze ontwikkelingen op automatiseringsgebied vragen erom die deskundigheid op peil te houden.

CRYPTOGRAFISCHE BEVEILIGING VAN ELEKTRONISCH BERICHTEN- EN BETALINGSVERKEER

door drs. T.P. de Vries

Inleiding

Enige toepassingen van elektronisch berichtenverkeer zijn electronic mail en elektronische documentuitwisseling.
Elektronische documentuitwisseling (of "EDI" -Electronic Data Interchange) heeft betrekking op het elektronisch verzenden van handelsdocumenten, zoals orders, facturen, betalingsopdrachten en dagafschriften. Betalingstransacties die via datacommunicatie worden verricht, zijn een bijzondere vorm van elektronisch berichtenverkeer.

Het doel van dit artikel is om aan te geven welke beveiligingsmechanismen kunnen worden geïnstalleerd om elektronisch berichtenverkeer te beschermen. Gezien de kritische aard van betalingstransacties zijn beveiligingsmaatregelen van groot belang voor deze toepassing van elektronisch berichtenverkeer.

In dit artikel zal eerst worden ingegaan op de mogelijke bedreigingen voor het elektronisch berichtenverkeer. Vervolgens worden de basiseigenschappen van de beveiligingstechniek - Data-Encryptie - besproken. Besloten wordt met een beschrijving van de hier behandelde maatregelen die getroffen kunnen worden tegen de eerder geïnventariseerde bedreigingen.

Door het toenemend gebruik van netwerken voor de transmissie van waardegegevens, de toename van de waarde van deze gegevens en de ingebruikneming van nieuwe technologieën zoals draadloze verzending van gegevens, wordt beveiliging van het elektronisch berichtenverkeer in toenemende mate noodzakelijk. Cryptografie is de enige bekende praktische en effectieve methode om deze informatie te beschermen. Tevens kan cryptografie op een zeer economische wijze worden aangewend.

In dit artikel wordt aangenomen dat de datatransmissie-media bij de aangeslotenen eindigen in een veilige omgeving. Methoden en technieken voor gebruikersauthenticatie en toegangscontrole blijven derhalve buiten beschouwing.

De aanname dat de eindpunten van de communicatiemedia zich in een veilige omgeving bevinden, betekent overigens niet dat de deelnemende partijen zijn te vertrouwen. Het is mogelijk dat een deelnemende partij zijn betrouwbare systeem op frauduleuze wijze gebruikt.
Er wordt daarom onderscheid gemaakt tussen een aanval en een fraude. Een aanval wordt uitgevoerd door een derde partij waarbij deze de berichtenstroom observeert of beïnvloedt. Fraude wordt gezien als een niet-wettige handeling door één of meerdere van de deelnemende partijen.

Een andere aanname is dat een aanvaller in staat is geweest zich toegang te verschaffen tot het communicatiepad tussen twee aangesloten partijen op het netwerk. De indringer heeft hierbij de beschikking over voldoende apparatuur- en datacommunicatiekennis om een aanval op een onvoldoende beveiligde transmissie uit te voeren.

Bedreigingenmodel

De mogelijke bedreigingen voor het elektronisch berichtenverkeer kunnen op de volgende wijze worden geclassificeerd [VoKe83]:

I passieve aanvallen:
   a. vrijkomen van de berichtinhoud;
      de aanvaller neemt kennis van de berichtinhoud;
   b. analyse van het berichtenverkeer;
      de aanvaller observeert de berichtenstroom en kan hierdoor kennis verkrijgen over de afzender, de bestemming, de lengte van de berichten en de frequentie van verzending;

II actieve aanvallen:
   a. het modificeren van de berichtenstroom;
      - inbreuk op de integriteit[1] van de berichtinhoud;
      - inbreuk op de authenticiteit[2] van de bron;
      - inbreuk op de volgorde binnen een bericht;
   b. het vertragen of onderdrukken van de gehele berichtenstroom;
   c. het initiëren van een namaakverbinding;
      - het tot stand brengen van een frauduleuze verbinding onder een valse identiteit;
      - hertransmissie van een voorgaand legitiem bericht;

III fraude door een deelnemende partij:
   a. ontkennen van berichtverzending en beweren van berichtontvangst;
   b. ontkennen van berichtontvangst en beweren van berichtverzending.

In dit artikel wordt niet ingegaan op onopzettelijk opgetreden fouten. Er is van uitgegaan dat deze fouten worden opgemerkt en waar mogelijk verholpen door, in het datacommunicatieprotocol opgenomen, error detection-technieken. Overigens kunnen maatregelen welke getroffen zijn om berichtmodificatie op te merken tevens onopzettelijke wijzigingen detecteren. Zij zijn er echter niet op gericht deze te verhelpen.

Passieve aanvallen

Passieve aanvallen zijn niet gericht op het beïnvloeden van de getransporteerde gegevens. De indringer neemt slechts kennis van de berichtenstroom die passeert maar tast deze niet aan. Het aspect vertrouwelijkheid wordt door deze aanvallen bedreigd.

Passieve aanvallen kunnen over het algemeen niet worden gedetecteerd. Aan het bericht zelf is immers niet te zien of er onbevoegd kennis van is genomen. Daarom zijn repressieve maatregelen niet bruikbaar en moet worden gekozen voor preventieve maatregelen.

De indringer kan ook kennis nemen van de oorsprong en de bestemming van de berichten, de frequentie waarmee berichten worden verzonden of de lengte van de berichten. Hieraan kan hij dan bij afwijkend gedrag conclusies verbinden. De indringer behoeft bij de analyse van het berichtenverkeer geen kennis te nemen van de inhoud van het bericht.

Actieve aanvallen

Actieve aanvallen zijn gericht op de beïnvloeding van de getransporteerde gegevens. Het aspect betrouwbaarheid wordt dan ook door dit soort aanvallen bedreigd.

Actieve aanvallen kunnen over het algemeen niet worden voorkomen. Alleen fysieke maatregelen kunnen preventief werken tegen actieve aanvallen. Dergelijke maatregelen zijn over het algemeen

---

1 Integriteit: Een integer bericht is een bericht dat in ongeschonden toestand de ontvanger bereikt.

2 Authenticiteit: Een authentiek bericht is een bericht dat van de opsteller zelf afkomstig is.

onpraktisch en oneconomisch. Alleen repressieve maatregelen kunnen worden gebruikt om achteraf de betrouwbaarheid[1] van de berichten vast te stellen.

Het modificeren van de berichtenstroom

Inbreuk op de integriteit van de berichtinhoud betekent dat een aanvaller de inhoud van het bericht tijdens transmissie heeft gewijzigd.

Inbreuk op de authenticiteit van de bron daarentegen betekent dat niet onomstotelijk kan worden vastgesteld of het ontvangen bericht afkomstig is van de geautoriseerde verzender aan de andere kant van het communicatiemedium.

Berichten of delen van berichten kunnen door een aanvaller selectief worden verwijderd, verdubbeld, toegevoegd of in een andere volgorde gezet. Dit heeft een inbreuk op de berichtvolgorde tot gevolg.

Het vertragen of onderdrukken van de gehele berichtenstroom

In deze soort van actieve aanval vertraagt of onderdrukt de aanvaller alle berichten die op een verbinding passeren. De aanvaller modificeert de berichtinhoud op geen enkele wijze maar probeert voordeel te halen uit de vertraging of onderdrukking van de berichtenstroom.

In veel gevallen zal de verzender van de gegevens een dergelijke aanval opmerken maar geen mogelijkheden hebben om de bedoelde ontvanger via de gebruikte verbinding op de hoogte te stellen aangezien deze wordt beïnvloed door de aanvaller.

Het initiëren van een namaakverbinding

In de derde vorm van actieve aanvallen herzendt de aanvaller een eerder afgetapt en opgenomen legitiem bericht. Een tweede mogelijkheid is dat de aanvaller een frauduleuze verbinding onder een valse identiteit tot stand probeert te brengen.

Om het initiëren van een namaakverbinding te voorkomen is het noodzakelijk dat de hard- en software-configuraties van beide eindpunten zich op een veilige wijze wederzijds authenticeren.

Fraude vanuit de betrokken gebruikers

Het is niet noodzakelijk dat de bedreigingen voor het elektronisch berichtenverkeer afkomstig zijn van een derde onafhankelijke indringer. Een aanval kan ook door één of meerdere van de aangesloten partijen worden uitgevoerd. In dit geval is er sprake van een meer indirecte aanval, aangezien de communicatiemedia op geen enkele wijze fysiek of logisch beïnvloed of afgetapt worden. Daarom is gekozen om in dit geval te spreken over fraude.

De vier volgende fraudegevallen zijn te onderscheiden:
- (onterecht) ontkennen van berichtverzending door de authentieke verzender;
- (onterecht) beweren van berichtontvangst door de authentieke ontvanger;
- (onterecht) ontkennen van berichtontvangst door de authentieke ontvanger;
- (onterecht) beweren van berichtverzending door de authentieke verzender.

Beschikbare technieken

De in dit artikel behandelde beveiligingsmaatregelen tegen de hiervoor genoemde bedreigingen zijn gebaseerd op encryptiemethodieken. In dit hoofdstuk wordt ingegaan op de basisprincipes van de conventionele encryptie-algoritmen, de Public Key encryptie-algoritmen en de Key Management-methoden.

---

1 Betrouwbaarheid: Een betrouwbaar bericht is een bericht waarvan de integriteit, de authenticiteit en de volgorde is gewaarborgd.

De encryptie-algoritmen en hun (on)mogelijkheden

De invoer van de vercijferfunctie van een encryptie-algoritme wordt "plaintext" of "klare tekst" genoemd. Het resultaat van de vercijfering is de "ciphertext" of "vercijferde tekst". Een tweede parameter voor het vercijferalgoritme is de sleutel. Het vercijferalgoritme heeft een bijbehorende inverse operatie - het ontcijferalgoritme - welke, indien de correcte sleutel wordt aangeboden en toegepast op de ciphertext, de correcte plaintext oplevert.

In civiele toepassingen wordt momenteel uit oogpunt van standaardisatie en robuustheid voornamelijk gebruik gemaakt van encryptie-algoritmen waarvan het algoritme publiek bekend is. Dit betekent dat de betrouwbaarheid van een dergelijk algoritme berust op de geheimhouding van de sleutels. Er worden twee soorten van encryptie-algoritmen onderscheiden; het symmetrische encryptie-algoritme en het asymmetrische encryptie-algoritme.

Symmetrische algoritmen

Het kenmerk van de conventionele algoritmen is dat de sleutel voor ontcijfering gelijk is aan de sleutel voor vercijfering. Deze algoritmen worden daarom ook wel symmetrische encryptie-algoritmen genoemd. De encryptie-sleutel dient geheim te zijn en alleen te kunnen worden gebruikt door de geautoriseerde gebruikers.

De "Data Encryption Standard", kortweg DES, is een voorbeeld van een conventioneel algoritme.

Het DES-algoritme is een zogenaamd "blokcijfer" wat betekent dat het een invoer van 64 bits per encryptie/decryptie kan vercijferen/ontcijferen. Over het algemeen zal een bericht echter bestaan uit meerdere gegevensblokken van 64 bits. Gegevensblokken met gelijke inhoud resulteren na vercijfering met dezelfde sleutel in vercijferde blokken met dezelfde inhoud. Dit betekent dat gegevenspatronen met een bloklengte die precies binnen de blokgrenzen vallen, kunnen worden herkend. Deze mogelijkheid van patroonherkenning kan worden voorkomen door gebruik te maken van een geschikte wijze van gebruik van het data-encryptie-algoritme. Bij DES kunnen daarom verschillende encryptiemodes gebruikt worden om de gegevens te vercijferen.

In het geval dat een bericht bloksgewijs (64 bits) met DES wordt encrypt, spreekt men van Electronic Code Book (ECB). Bij deze encryptiemode is dus geen sprake van het maskeren van gegevenspatronen. Andere encryptiemodes bezitten deze eigenschap wel.

Encryptiemodes kunnen naast de patroonversluieringseigenschap tevens beschikken over de eigenschappen foutvoortplanting of zelfsynchronisatie.

Indien gebruik wordt gemaakt van een encryptiemode met foutvoortplanting zal verandering van een bit van de ciphertext de mogelijkheid voor de ontvanger om het bericht correct te ontcijferen, beïnvloeden: de ontcijferde plaintext zal, vanaf het gegevensblok waar de fout in de ciphertext optrad, zijn aangetast.

Een zelfsynchroniserend schema is dusdanig geconstrueerd, dat als er een fout optreedt in een blok van de ciphertext, deze fout zichzelf herstelt. De fout plant zichzelf dus niet voort in de volgende blokken. Dit wil zeggen dat alle plaintext correct kan worden herwonnen met uitzondering van dat deel dat direct door de fout werd aangetast.

Een toepassing voor een schema met zelfsynchronisatie is de encryptie van bestanden die moeten worden opgeslagen. Hierdoor blijft een eventuele fout beperkt tot een klein gebied in de herwonnen plaintext en is herstel van deze fout meestal nog mogelijk.

Asymmetrische algoritmen

In tegenstelling tot het symmetrische data encryptie-algoritme is het vercijferproces bij Public Key-algoritmen verschillend van het ontcijferproces [DiHe76]. Dit wordt bereikt door gebruik te maken

van een sleutelpaar (SK, PK). Public Key-algoritmen bieden de mogelijkheid dat één van beide sleutels (PK) openbaar wordt gemaakt, terwijl de andere sleutel (SK) geheim dient te blijven. Elk van deze sleutels behoort bij een transformatie welke elkaars inverse zijn. Kennis van de publieke sleutel PK mag er niet toe leiden dat de geheime sleutel SK kan worden berekend. Een met één van beide sleutels vercijferde plaintext kan niet met behulp van dezelfde sleutel worden ontcijferd.

Een Public Key-algoritme kan op twee manieren worden gebruikt:
1. voor de versluiering van het bericht, zodat de vertrouwelijkheid van het bericht wordt gewaarborgd;
2. voor het genereren van een zogenaamde Digitale Handtekening[1] waarmee de authenticiteit van de verzender van het bericht en de integriteit van de berichtinhoud kan worden vastgesteld.

Ad 1

Een deelnemende partij A maakt aan deelnemer B op het netwerk bekend dat hij een (vertrouwelijk) bericht M wil sturen. Deelnemer B genereert vervolgens een sleutelpaar (SKb, PKb). De publieke sleutel PKb, die voor iedereen bekend mag zijn, wordt vervolgens aan A verstrekt. Deelnemer A past vervolgens de encryptie-operatie E onder de sleutel PKb op het bericht M toe. Het resultaat is het vercijferde bericht $E_{PKb}(M)$[2]. A zendt het vercijferde bericht naar B.
Aangezien de vercijfersleutel PKb voor een ieder bekend mag zijn, kan iedereen een boodschap versleutelen, echter alleen de bezitter B van de geheime sleutel SKb is in staat de boodschap te ontcijferen.

Ontvanger B is er echter niet zeker van dat het ontvangen vercijferde bericht ook werkelijk van A afkomstig is. Immers iedereen kan de publieke sleutel PKb gebruiken om een bericht te vercijferen. Er is daarom een mechanisme nodig dat een zender identificeert (zie ad 2).

Het is mogelijk dat een indringer C een sleutelpaar (SKc, PKc) genereert, de publieke sleutel PKc aan A verstrekt (als ware deze van B afkomstig) en vervolgens het door A verzonden en met PKc encrypte bericht opvangt en kennis neemt van de inhoud van het bericht door het te ontcijferen met SKc. Om dit te voorkomen, is er een mechanisme nodig dat de verzender A de authenticiteit van de publieke sleutel PKb garandeert (zie Public Key Sleutel Distributie Centrum).

Ad 2

A beschikt over een eigen geheime sleutel SKa. De bijbehorende publieke sleutel PKa is algemeen bekend. De distributie van de publieke sleutel PKa is uitgevoerd op een zodanige wijze dat B er zeker van is dat hij beschikt over de authentieke PKa (zie Public Key Sleutel Distributie Centrum).

Als A een bericht naar B zendt, dan past A de decryptie-operatie op het bericht toe onder de eigen geheime sleutel SKa en zendt het resultaat, het cryptogram $D_{SKa}(M)$, naar B.

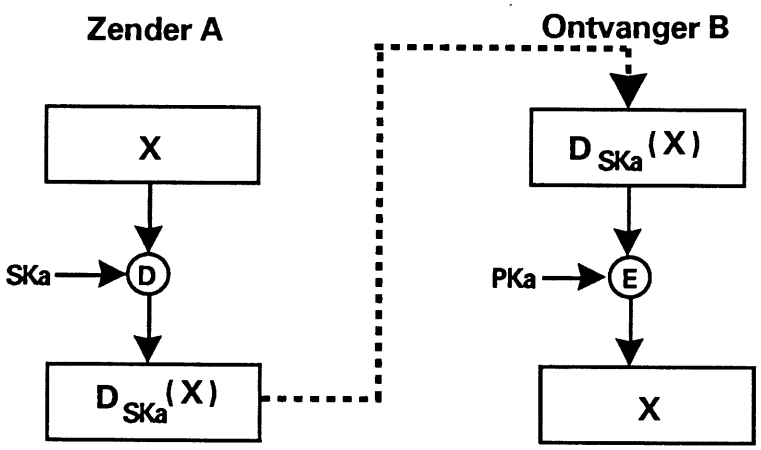
Decryptie met SKa draagt niet bij tot de geheimhouding van het bericht M (daar iedereen die beschikt over de openbare sleutel PKa het bericht kan ontcijferen), maar bewijst dat het bericht door A verzonden is (daar alleen A de geheime sleutel heeft) en tijdens transport onveranderd is gebleven.

B kan ook aan derden bewijzen dat het bericht van A afkomstig moet zijn. B geeft hiervoor het cryptogram $D_{SKa}(M)$ af aan de beoordelende partij C.
C kan met PKa vaststellen dat het bericht van A afkomstig moet zijn. Immers A is de enige die beschikt over SKa.

---

1 Voor het mogelijk gebruik van een Digitale Handtekening wordt geëist dat: $E_{PK}(D_{SK}(X)) = X$.

2 $E_{PK}(X)$: Encryptie-operator E werkt onder de publieke sleutel PK op de operand X.
$D_{SK}(Y)$: Decryptie-operator D werkt onder de geheime sleutel SK op de operand Y.



Authenticatie afzender en bericht-integriteit met een Public Key-algoritme.

Merk op:
Eventueel kan A besluiten om het bericht na decryptie met SKa, tevens te encrypten met PKb. De encryptie met PKb draagt bij tot de geheimhouding van M, want alleen B is nu in staat het bericht te lezen door het ontvangen bericht eerst te decrypten met zijn geheime sleutel SKb en het resultaat vervolgens te encrypten met PKa. A weet dus dat alleen B het bericht kan lezen en B weet dat het bericht van A afkomstig is en kan vaststellen dat het onveranderd is gebleven.

Public Key Sleutel Distributie Centrum

Wil ontvanger B met zekerheid vaststellen dat het bericht van de authentieke verzender A afkomstig is, is het noodzakelijk dat hij kan steunen op de authenticiteit van de, door A aan B verstrekte, publieke sleutel PKa.
Indien dit niet gebeurt, is het mogelijk dat een frauduleuze partij C een Public Key-sleutelpaar (SKc, PKc) genereert, de publieke sleutel PKc aan B verstrekt en een frauduleus bericht met SKc van een Digitale Handtekening voorziet (zie Asymmetrische algoritmen ad 2).

Ook indien de vertrouwelijkheid van een bericht moet worden gegarandeerd is het noodzakelijk dat de verzender A van het bericht de authenticiteit van de aan hem verstrekte publieke sleutel PKb kan vaststellen (zie Asymmetrische algoritmen ad 1).

De noodzaak voor de authenticatie van de publieke sleutels geeft aanleiding om gebruik te maken van een Public Key Sleutel Distributie Centrum voor het op veilige wijze distribueren van de gebruikte sleutels. Hierdoor wordt een van de vermeende voordelen van Public Key-systemen boven conventionele systemen, de vereenvoudigde sleuteldistributie, gedeeltelijk tenietgedaan.

RSA

Eén van de Public Key-algoritmen, het RSA-algoritme (de voorletters van de namen van de ontwikkelaars, Rivest, Shamir en Adleman [RiSh78]), is gebaseerd op een tot nog toe onopgelost wiskundig probleem, het zogenaamde factoriseringsprobleem. Factorisering is het uitsplitsen van een getal in priemgetallen, zodanig dat het produkt van deze priemgetallen het te factoriseren getal oplevert.

Een priemgetal is een getal dat slechts deelbaar is door 1 en het getal zelf. Een priemgetal kan dus niet worden gefactoriseerd. Tot nog toe is het niet gelukt een analytische methode te vinden waarmee snel een zeer groot getal kan worden gefactoriseerd.

Hier zal worden besproken hoe RSA kan worden toegepast.

Een Public Key-algoritme moet aan de volgende voorwaarden voldoen:

1. een sleutelpaar (SK, PK) moet gemakkelijk zijn te berekenen;
2. SK mag niet eenvoudig uit PK zijn af te leiden;
3. $D_{SK}(E_{PK}(X))=X$.

Het Public Key-algoritme kan voor het zetten van Digitale Handtekeningen worden gebruikt indien tevens geldt:

$E_{PK}(D_{SK}(X))=X$ voor alle X in het domein van D_{SK}.

Om RSA te kunnen toepassen, zijn twee zeer grote priemgetallen p en q nodig ($p \neq q$). Er bestaan verschillende algoritmen om vast te stellen of een (groot) getal een priemgetal is. De priemgetallen p en q worden geheimgehouden.

Als twee priemgetallen p en q zijn verkregen, worden de waarde r (welke niet geheim behoeft te blijven) en de Euler functiewaarde $\phi(r)$ (welke geheim moet blijven) als volgt berekend:

$r = p*q$ en $\phi(r) = (p-1)*(q-1)$

$\phi(r)$ geeft het aantal getallen aan dat relatief priem[1] is met r en kleiner dan r.

De PK wordt gekozen zodanig dat PK relatief priem is met $\phi(r)$.
De geheime sleutelwaarde SK wordt bepaald zodanig dat voldaan wordt aan de volgende vergelijking:

$PK*SK = 1 \bmod \phi(r)$. [2]

De encryptie-operatie wordt gedefinieerd als:

$Y = E_{PK}(X) = X^{PK} \bmod r$ met $X \in \{0, 1, ...,r-1\}$

en de decryptie-operatie als:

$X = D_{SK}(Y) = Y^{SK} \bmod r$ met $Y \in \{0, 1, ...,r-1\}$.

Een methode om RSA te breken is om r te factoriseren zodat p, q en $\phi(r)$ bekend worden en SK uit $PK*SK = 1 \bmod \phi(r)$ is af te leiden. Wiskundigen zijn er in geslaagd een getal van circa 90 cijfers te factoriseren in twee grote priemwaarden. Hiervoor werd gebruik gemaakt van een vector-computer. Een veilig cryptografisch algoritme behoort met een veel groter getal te werken. Momenteel wordt een lengte van 512 bits (154 cijfers) voor de modulus r als voldoende beschouwd.

Key Management

De beveiliging van het systeem berust op de geheimhouding van de sleutels. Om dit te bereiken moet bijzondere aandacht worden besteed aan de generatie, distributie, vervanging, beveiliging, opslag en vernietiging van de sleutels. Key Management dient erin te voorzien dat de geheimhouding van de sleutels kan worden gewaarborgd en dat bij onverhoopt openbaar worden van een sleutel de gevolgen zoveel mogelijk beperkt blijven.

De belangrijkste eisen die aan het Key Management gesteld worden zijn:
- sleutels moeten gegenereerd worden met behulp van een random of pseudo-random proces;
- elke sleutel die door twee communicerende knooppunten gebruikt wordt moet voor deze knooppunten uniek zijn;
- een sleutel dient slechts voor één doeleind gebruikt te worden, dat wil zeggen dat dezelfde sleutel niet mag worden gebruikt voor het bereiken van zowel vertrouwelijkheid als integriteit;

---

1 Relatief priem; Twee gehele positieve getallen a en b zijn relatief priem als de grootste gemene deler van a en b gelijk is aan 1.

2 $a=b \bmod m$; Het verschil a-b van de gehele getallen a en b is deelbaar door het gehele getal m. Dat wil zeggen, er is een geheel getal k zodanig dat $a = b + k * m$.

- elke sleutel moet, binnen de tijd dat deze achterhaald kan worden, worden vervangen;
- een sleutel waarvan bekend is of vermoed wordt dat hij gecompromitteerd is, dient vervangen te worden;
- compromittering van een sleutel die door twee partijen gedeeld wordt mag niet leiden tot de compromittering van een sleutel van een derde partij;
- sleutels mogen alleen in klare vorm voorkomen in een fraude-ongevoelige cryptografische eenheid. Elders dienen alle sleutels vercijferd te zijn of uit meerdere componenten te bestaan.

De toewijzing en bescherming van sleutels is hiërarchisch georganiseerd. De grote hoeveelheid gegevens wordt beschermd door een kleiner aantal dynamisch gegenereerde Data Encryption Keys (DEK). De Data Encryption Keys worden beschermd door een nog kleiner aantal relatief constante Key Encryption Keys (KEK). Op hun beurt worden de Key Encryption Keys vercijferd onder de host Master Key of varianten daarvan.

Bijgevolg behoeft slechts een klein aantal sleutels in klare vorm in een fraude-ongevoelige cryptografische eenheid te worden opgeslagen, de zogenaamde Tamper Resistant Security Module. Alle andere sleutels kunnen in vercijferde vorm worden opgeslagen. De instructieset van een Tamper Resistant Security Module is zodanig dat het onmogelijk is om de klare waarde van een sleutel te distilleren ongeacht de invoer voor de Tamper Resistant Security Module en de volgorde waarin de basisoperaties worden uitgevoerd.

Indien een Data Encryption Key (DEK) alleen actief is gedurende een enkele communicatiesessie, spreekt men van een sessiesleutel. De sessiesleutels worden bij de verzendende deelnemer gegenereerd en vervolgens naar de ontvangende deelnemer gezonden.
Hierbij is de sessiesleutel vercijferd onder de Key Encryption Key (KEK). De per ontvangende deelnemer unieke Key Encryption Key wordt van tevoren geïnstalleerd. Hierdoor zal bij compromittering van een enkele Key Encryption Key de beveiliging van het gehele systeem niet in gevaar komen, maar beperkt blijven tot de deelnemende partij waarvan de Key Encryption Key openbaar is geworden.

Indien een sleutel voor de beveiliging van het gehele systeem van belang is, spreekt men van een globale sleutel.

Key Encryption Keys worden geheim gehouden door ze te vercijferen met een Master Key. Hierdoor is het mogelijk een groot aantal Key Encryption Keys te beheersen. De Key Encryption Keys worden vercijferd opgeslagen in de Key Table op secondary storage. De Master Key wordt geheim gehouden door ze op te slaan in een Tamper Resistant Security Module.

Het is ook mogelijk de sessiesleutel niet uit te wisselen door middel van encryptie onder een Key Encryptie Key maar deze per transactie bij de ontvangende en verzendende partij op separate wijze te laten aanpassen. We spreken dan over Transaction Key Management.

Dit houdt in dat bij het begin van iedere transactie, een nieuwe Transaction Key wordt berekend met behulp van de Terminal Key (opgeslagen in het sleutelregister van de transactie initiërende partij) en waarden bepaalt uit gegevens van het transactiebericht. Elke transactie is opgebouwd uit een aanvraagbericht (van transactie initiërende partij naar transactie verwerkende partij) en een antwoordbericht (van transactie verwerkende partij naar transactie initiërende partij).
Na afloop van iedere transactie wordt een nieuwe Terminal Key gegenereerd. De nieuwe Terminal Key is een functie van het MAC-residu[1] van het aanvraagbericht, het MAC-residu van het antwoordbericht en van de huidige Terminal Key.
Deze MAC-residuen worden gelijktijdig bepaald met de berekening van de MAC's voor de authenticatie van het aanvraag- en het antwoordbericht. De MAC's worden slechts voor de helft met de berichten meegezonden. De andere helft, het MAC-residu, wordt bewaard door de verzender. De ontvanger verifieert de integriteit van het bericht door de meegezonden MAC-waarde

1 Bij het bepalen van een Message Authentication Code (MAC) wordt een 64-bits getal, het zogenaamde Message Authentication Block (MAB), berekend. Slechts 32-bits worden gebruikt voor de MAC, de overige 32-bits worden het MAC-residu genoemd.

te vergelijken met de opnieuw berekende MAC-waarde. Door deze berekening heeft de ontvanger tevens de beschikking gekregen over het MAC-residu.

Na verzending en ontvangst van aanvraagbericht en antwoordbericht beschikken zowel de transactie initiërende partij als de transactie verwerkende partij over de MAC-residuen van beide berichten en zijn daarmee separaat in staat de volgende Terminal Key te genereren.

De voordelen van Transaction Key Management zijn:
- transactiesleutels onvoorspelbaar en automatisch gegenereerd;
- verkleining van communicatie overhead;
- bij het openbaar worden van de transactiesleutel blijft het risico tot de corresponderende transactie beperkt.

De nadelen zijn:
- de problemen bij verlies van synchronisatie;
- de (her)initialisatie.

Maatregelen

Hieronder zullen maatregelen worden besproken die tegen de onderkende bedreigingen kunnen worden genomen.

Voorkomen van passieve aanvallen

Voorkomen van het vrijkomen van de berichtinhoud en berichtanalyse

De hoeveelheid informatie die kan worden verborgen is afhankelijk van de OSI-laag waarin de encryptie plaatsvindt. In het geval de encryptie in laag N plaatsvindt, is de protocolinformatie uit laag N-1 en lager zichtbaar voor een indringer.

Het is mogelijk een enkele sleutel per groep van aangesloten deelnemers te gebruiken. Indien deze sleutel echter bekend raakt, zal de beveiliging van het berichtenverkeer van de gehele groep gecompromitteerd zijn. Anderzijds is de taak van sleuteldistributie vereenvoudigd. Dit in tegenstelling tot het gebruik van één unieke sleutel per deelnemerspaar, waar de gevolgen van het openbaar worden van de sleutel tot het deelnemerspaar beperkt blijven.

Een geschikte encryptiemode moet worden gebruikt om te voorkomen dat patronen in de blok-opbouw worden herkend en misbruikt. De ECB-mode is dus ongeschikt.

De protocollaag waarin de encryptie plaatsvindt, legt de precisie vast waarmee berichtanalyse mogelijk is. Hoe lager encryptie in het lagenmodel plaatsvindt, hoe meer gegevens voor de eventuele indringer verborgen blijven. Er worden echter grenzen gesteld aan de haalbaarheid van sommige maatregelen omdat zij van te grote invloed zijn op effectieve bandbreedte van het netwerk en een te grote invloed hebben op de verwerkingscapaciteit van de hosts.

Voor End-to-End-beveiliging zal encryptie in de applicatie-, presentatie-, sessie- of transportlaag moeten plaatsvinden. Dit betekent dat een eventuele aanvaller een berichtanalyse kan uitvoeren.

Bij Link-encryptie moet encryptie in de Data Link-laag plaatsvinden. Hierdoor worden berichtanalyses voorkomen. Link-encryptie geeft echter mogelijkheden voor een aanval in de knooppunten waar decryptie en encryptie moet plaatsvinden. Dit betekent dat de hard- en software-componenten in de tussenliggende knooppunten moeten worden gecertificeerd en de knooppunten zich in een veilige omgeving moeten bevinden.

In veel gevallen zullen de netwerkgebruikers niet willen steunen op de beveiligingsmaatregelen die door de tussenliggende knooppunten worden geboden.

Vaststellen van actieve aanvallen

Vaststellen van de modificatie van de berichtenstroom

De belangrijkste maatregelen die tegen modificatie van de berichtenstroom genomen kunnen worden zijn gericht op het vaststellen van de integriteit. De maatregelen die de authenticiteit van de bron vaststellen, zijn gebaseerd op de integriteitsmaatregelen. De maatregelen voor de vaststelling van de correcte berichtvolgorde berusten op zowel berichtintegriteits- als bronauthenticiteitsmaatregelen.

De integriteitsmaatregelen hebben tot doel om de ontvanger de mogelijkheid te bieden om vast te stellen of een bericht is gewijzigd gedurende het transport.

Het vaststellen van de authenticiteit wordt mogelijk door elk bericht uniek en onveranderbaar aan de verbinding te koppelen. Dit wordt bereikt door het gebruik van een separate sleutel per verbinding. Indien meerdere verbindingen dezelfde sleutel gebruiken, moet een afzonderlijke identificatie per verbinding worden gebruikt.

De vaststelling of onderdelen van een bericht in de goede volgorde zijn ontvangen wordt mogelijk door het gebruik van unieke volgorde-afhankelijke waarden per berichtonderdeel. Pogingen om de volgorde-afhankelijke waarde te wijzigen moeten worden opgemerkt door de toegepaste integriteitsmaatregel.

Berichtintegriteit

Gebruikers en applicatieprogramma's zullen veranderingen in een bericht niet altijd ontdekken. De kans dat deze veranderingen worden opgemerkt wordt vergroot indien een encryptie-schema met foutvoortplanting wordt toegepast. Echter, veel applicatieprogramma's zijn niet ontworpen om dergelijke veranderingen te detecteren. Het detecteren van veranderingen door elke applicatie afzonderlijk zal leiden tot onnodig compliceren van de integriteitsmaatregelen.

In de meeste cryptografische toepassingen is meer behoefte aan de handhaving van de integriteit van de berichtinhoud dan aan het waarborgen van de vertrouwelijkheid. Als de zender achter het bericht een error detection code toevoegt, kan de ontvanger de integriteit van het bericht vaststellen.

Berichtintegriteit stelt de ontvanger in staat de afkomst, de bestemming, de inhoud, de tijdigheid en de volgorde van een bericht te toetsen op hun geldigheid. Hiervoor zal het bericht moeten worden aangevuld met een tijdafhankelijke waarde en/of een volgnummer. Het gebruik van een unieke geheime sleutel door de zender en ontvanger stelt de ontvanger in staat de authenticiteit van de bron en de bestemming te valideren.

In het vervolg van het artikel zal worden aangenomen dat onder het "bericht" wordt verstaan het oorspronkelijke bericht aangevuld met tijd en/of volgorde-afhankelijke waarden.

Bekende hulpmiddelen die gebruikt kunnen worden om de integriteit van de berichtinhoud te kunnen waarborgen zijn:
- Manipulation Detection Code;
- Message Authentication Code;
- Digitale Handtekening.

De belangrijkste verschillen tussen bovenstaande hulpmiddelen en hun toepassingsgebieden zullen worden besproken. De Digitale Handtekening is reeds beschreven in de sectie "Asymmetrische algoritmen".

Message Authentication Code

Een Message Authentication Code (MAC) is een waarde (32-bits) die berekend wordt met behulp van het DES-algoritme uit de gehele berichtinhoud en een geheime sleutel. Met een MAC kan de integriteit van een bericht worden vastgesteld zonder dat de vertrouwelijkheid van dat bericht is gewaarborgd. De wijze waarop de MAC moet worden berekend, is vastgelegd in de standaard ANSI X9.9.

Als de zender aan het bericht een Message Authentication Code toevoegt, kan de ontvanger de integriteit van het bericht vaststellen. Indien het bericht geheim dient te worden gehouden, dient het bericht tevens te worden vercijferd met een andere sleutel.
De ontvanger stelt de integriteit van het bericht vast door de MAC te herberekenen en te vergelijken met de meegezonden MAC-waarde. Hij dient hiervoor te beschikken over dezelfde geheime sleutel als de verzender.
Mocht er een verandering optreden op het traject zender-ontvanger dan zal de uit het ontvangen bericht herberekende MAC-waarde verschillen van de met het bericht meegezonden MAC-waarde.

De betrouwbaarheid van een MAC berust op de geheimhouding van de sleutel. Indien de sleutel wordt gecompromitteerd is het mogelijk de plaintext te manipuleren zonder dat de oude MAC-waarde wordt gewijzigd. Om de integriteit van het bericht te handhaven volstaat het niet om de integriteit van de MAC te waarborgen.

Manipulation Detection Code

De Manipulation Detection Code (MDC) is een functie van de inhoud van het bericht waarvan de integriteit moet worden gewaarborgd [JuMa83].
Er wordt van uitgegaan dat de MDC-functie publiek bekend is. Dit betekent dat de noodzakelijke integriteit van de MDC-waarde kan worden bereikt door het bericht geconcateneerd met de bijbehorende MDC met een geheime sleutel te vercijferen. Waarmee tevens de vertrouwelijkheid van de berichtinhoud is gewaarborgd.

Afwijkingen van deze opzet zijn mogelijk. Zo kan bijvoorbeeld alleen de MDC en niet de data worden encrypt met een geheime sleutel, of kunnen de plaintext en de MDC-waarde separaat worden opgeslagen en/of verzonden.

Een MDC gebruikt dus een functie die geen geheime informatie nodig heeft. Dit wil zeggen dat de cryptografische sterkte niet afhankelijk is van de geheimhouding van het algoritme.

Hoewel het gebruik van een MAC (onder de voorwaarde van geheimhouding van de sleutel) security voordelen biedt boven het gebruik van sommige MDC's, kan besloten worden tot het gebruik van een MDC om het Key Management niet verder te compliceren.

Aan het gebruik van sommige Manipulation Detection Codes (MDC) in combinatie met de gebruikte DES encryptiemode kleven nadelen. Zo is aangetoond dat, voor een aantal MDC-technieken, manipulaties aan de vercijferde tekst niet in alle gevallen behoeven te leiden tot een verandering in de MDC-waarde en bijgevolg niet worden opgemerkt.

Een sterke MDC-algoritme is zodanig ontworpen dat het nagenoeg onmogelijk is de plaintext te wijzigen zonder dat de MDC-waarde wordt aangetast.
Om de integriteit van het bericht te handhaven volstaat het om de integriteit van de MDC te waarborgen.

Vaststellen van vertraging of onderdrukking van de gehele berichtenstroom

De maatregelen die gebruikt worden tegen berichtmodificatie kunnen in een aantal gevallen uitkomst brengen. Om een aanval of een aanvalspoging van dit type op een stille verbinding te kunnen detecteren, zal een vorm van vraag-antwoordmechanisme moeten worden toegepast.

Hierbij wordt periodiek een verzoek naar de andere partij gezonden waarop een antwoord wordt verwacht. Indien dit antwoord niet binnenkomt, wordt aangenomen dat een aanval plaatsvindt.

Vaststellen van het initiëren van een namaakverbinding

Om het tot stand brengen van een frauduleuze verbinding onder een valse identiteit te kunnen voorkomen moet het mogelijk zijn de authenticiteit van de identiteiten van de deelnemers vast te stellen. Het gebruik van een unieke sleutel per tweetal deelnemers zorgt impliciet voor deze authenticatie. Dit betekent dat de authenticatie tussen gebruikers berust op het gebruik van een geschikte sleuteldistributie en de geheimhouding van de sleutels.

Door te verifiëren dat de verbinding op hetzelfde moment tot stand wordt gebracht, is een maatregel tegen de hertransmissie van een voorgaand legitiem bericht genomen. Dit kan worden bereikt door het Challenge-Response-mechanisme. Zender en ontvanger zenden elkaar een random-waarde als Challenge. De andere zijde moet dan de vercijferde waarde van de Challenge als Response terugzenden. Bij ontvangst verifiëren beide zijden de Response door deze te ontcijferen en het resultaat te vergelijken met de referentiewaarde van de Challenge die verzonden was. Door het Challenge-Response-mechanisme bewijzen beide zijden aan elkaar in het bezit te zijn van de correcte encryptiesleutel.

Door dit mechanisme in het sleuteldistributiemechanisme te integreren, kan het aantal berichten worden verkleind.

Voorkomen van fraude door een deelnemende partij

Bij een symmetrisch algoritme zoals DES, waarbij zowel verzender als ontvanger over dezelfde sleutel beschikken, is het mogelijk dat:
- de verzender ontkent een bericht te hebben verzonden;
- de verzender beweert een bericht te hebben verzonden;
- de ontvanger beweert een bericht te hebben ontvangen;
- de ontvanger ontkent een bericht te hebben ontvangen.

Bewijslast tegen deze fraudemogelijkheden kan worden geboden door gebruik te maken van de Digitale Handtekeningmogelijkheid van een asymmetrisch algoritme en een geschikt protocol.

Er bestaat voor zover bekend nog geen jurisprudentie omtrent de vraag of een dergelijk schema ook in juridische zin een bewijs vormt.

Weerleggen van ten onrechte ontkennen van berichtverzending en ten onrechte beweren van berichtontvangst

Indien gebruik wordt gemaakt van een asymmetrisch algoritme en een Digitale Handtekening ($D_{SKa}(M)$) wordt geplaatst met de geheime sleutel van de verzender, is het niet mogelijk dat:
- de verzender ten onrechte de verzending van het bericht ontkent. De ontvanger kan deze ontkenning immers weerleggen met het, door de verzender, getekende bericht;
- de ontvanger ten onrechte beweert een bericht te hebben ontvangen. De ontvanger kan deze bewering immers niet aantonen met het, door de verzender, getekende bericht.

Weerleggen van ten onrechte ontkennen van berichtontvangst en ten onrechte beweren van berichtverzending

Indien elk bericht wordt bevestigd en het bevestigingsbericht wordt voorzien van een Digitale Handtekening (D_{SKb}(bevestiging b)) geplaatst met de geheime sleutel van de ontvanger, is het niet mogelijk dat:
- de ontvanger ten onrechte de ontvangst van het bericht ontkent. De verzender kan deze ontkenning immers weerleggen met de, door de ontvanger, getekende bevestiging;
- de verzender ten onrechte beweert een bericht te hebben verzonden. De verzender kan deze bewering immers niet aantonen met de, door de ontvanger, getekende bevestiging.

Slotopmerkingen

In dit artikel worden de risico's behandeld die het Electronisch Berichtenverkeer bedreigen. Tevens werd - op globale wijze - ingegaan op de beschikbare technieken en hoe deze kunnen worden toegepast om het optreden van deze bedreigingen te voorkomen of te detecteren.

Geen aandacht is besteed aan de benodigde organisatorische maatregelen om de technische maatregelen een voldoende stevige basis te geven om betrouwbaar te kunnen functioneren. Evenmin werd aandacht besteed aan de juridisch gezien benodigde bewijsmiddelen om een transactie te bewijzen of te ontkennen.

De organisatie die overweegt zijn elektronisch berichtenverkeer te gaan beveiligen, dient zich te realiseren dat de benodigde maatregelen afhankelijk zijn van de organisatie en de toepassing. Slechts na een grondige inventarisatie van de systeemeisen, risico-afweging en kosten/baten-analyse kan worden gekozen voor een effectief beveiligingspakket voor het elektronisch berichtenverkeer.

Ten slotte moet worden opgemerkt dat het tot op heden niet gelukt is een encryptie-algoritme te ontwikkelen waarvan wiskundig kan worden bewezen dat het met analytische methoden niet kraakbaar is. Een encryptie-algoritme waarvoor een analytische methode wordt gevonden om het te breken is onbruikbaar geworden. Een voordeel van niet geheime encryptie-algoritmen is dat research-centra over de gehele wereld de weerstand van het algoritme tegen analytische, statistische en deterministische aanvallen of een combinatie daarvan kunnen beproeven. Ondanks internationale research-inspanningen zijn tot op heden voor DES en RSA geen praktisch bruikbare kraakmethoden bekend.

Literatuuroverzicht

[VoKe83], Security Mechanisms in High-Level Network Protocols, V.L. Voydock and S.T. Kent, Computing Surveys, vol. 15, no. 2 June 1983.

[JuMa83], Message Authentication with Manipulation Detection Codes, R.R. Jueneman, S.M. Matyas, and C.H. Meyer, IEEE 1983.

A High Speed Manipulation Detection Code, R.R. Jueneman.

[RiSh78], A Method for Obtaining Digital Signatures and Public-Key Cryptosystems, R.L. Rivest, A. Shamir and L. Adleman, Communications of the ACM, 21, N0. 2, 120-126. (1978).

Cryptography: A new dimension in computer data security, Carl H. Meyer and Stephen M. Matyas, John Wiley & sons. (1982), ISBN 0-471-04892-5.

[DES], Data Encryption Standard, Federal Information Processing Standard Publication 46, National Bureau of Standards, U.S. Department of Commerce, Washington, D.C. (January 1977).

Exhaustive cryptanalysis of the NBS Data Encryption Standard, W. Diffie and M. E. Hellman, Computer, 10, 6, 74. (June 1977).

[DiHe76], New directions in cryptography, W. Diffie and M. Hellman, IEEE Transactions on Information Theory, 22, 644-645. (November 1976).

Security for computer networks, D.W. Davies and W.L. Price, John Wiley & sons. (1984), ISBN 0-471-90063 x.

Beveiligingsaspecten van computernetwerken, drs.ing. H.A.J.M. Spape RA, Compact zomer 1989, blz. 69-77.

S.W.I.F.T. EN CONTROLE

door drs. P.M. Knuvers en ing. G.H.M. Meijer

1 Inleiding

S.W.I.F.T. (hierna: SWIFT) staat voor "Society for Worldwide Interbank Financial Telecommunication". De SWIFT-organisatie is een coöperatie van banken, gevestigd te Brussel. De organisatie heeft tot doel het opzetten en onderhouden van een telecommunicatienetwerk voor het ontvangen, vastleggen, doorleveren en bezorgen van berichten in standaardformaat ten behoeve van de bij de internationale coöperatie aangesloten banken.

Het doel van dit artikel is het verschaffen van algemene informatie omtrent SWIFT, en het geven van handreikingen om in te schatten welke risico's met het gebruik van het SWIFT-netwerk samenhangen en hoe deze kunnen worden beheerst met behulp van een stelsel van maatregelen van interne controle en beveiliging. Dit stelsel van maatregelen is gericht op een betrouwbare en continue gegevensuitwisseling via het SWIFT-netwerk. Eveneens zal worden ingegaan op de werkzaamheden die in het kader van de controle van de jaarrekening met betrekking tot SWIFT moeten of kunnen worden uitgevoerd.

In hoofdstukken 2 en 3 wordt een beschrijving gegeven van de belangrijkste elementen van SWIFT, waarna in hoofdstuk 4 wordt ingegaan op de mogelijke bedreigingen. Vervolgens worden in hoofdstuk 5 de belangrijkste controlemaatregelen aangegeven. Door een bepaalde combinatie van deze maatregelen dient de betrouwbaarheid en continuïteit van de gegevensuitwisseling te worden gewaarborgd. Dit onderwerp wordt behandeld in hoofdstuk 6. In dit hoofdstuk wordt tevens aangegeven wanneer de EDP auditor kan participeren tijdens de controle van het buitenlands betalingsverkeer.

Dit artikel is hoofdzakelijk gerelateerd aan het, nog niet operationele, SWIFT II-netwerk. De opbouw hiervan verschilt op een aantal punten van het huidige SWIFT I-netwerk. Voor verdere informatie hieromtrent wordt verwezen naar hoofdstuk 7 ("Migratie van SWIFT I naar SWIFT II").

2 Algemeen

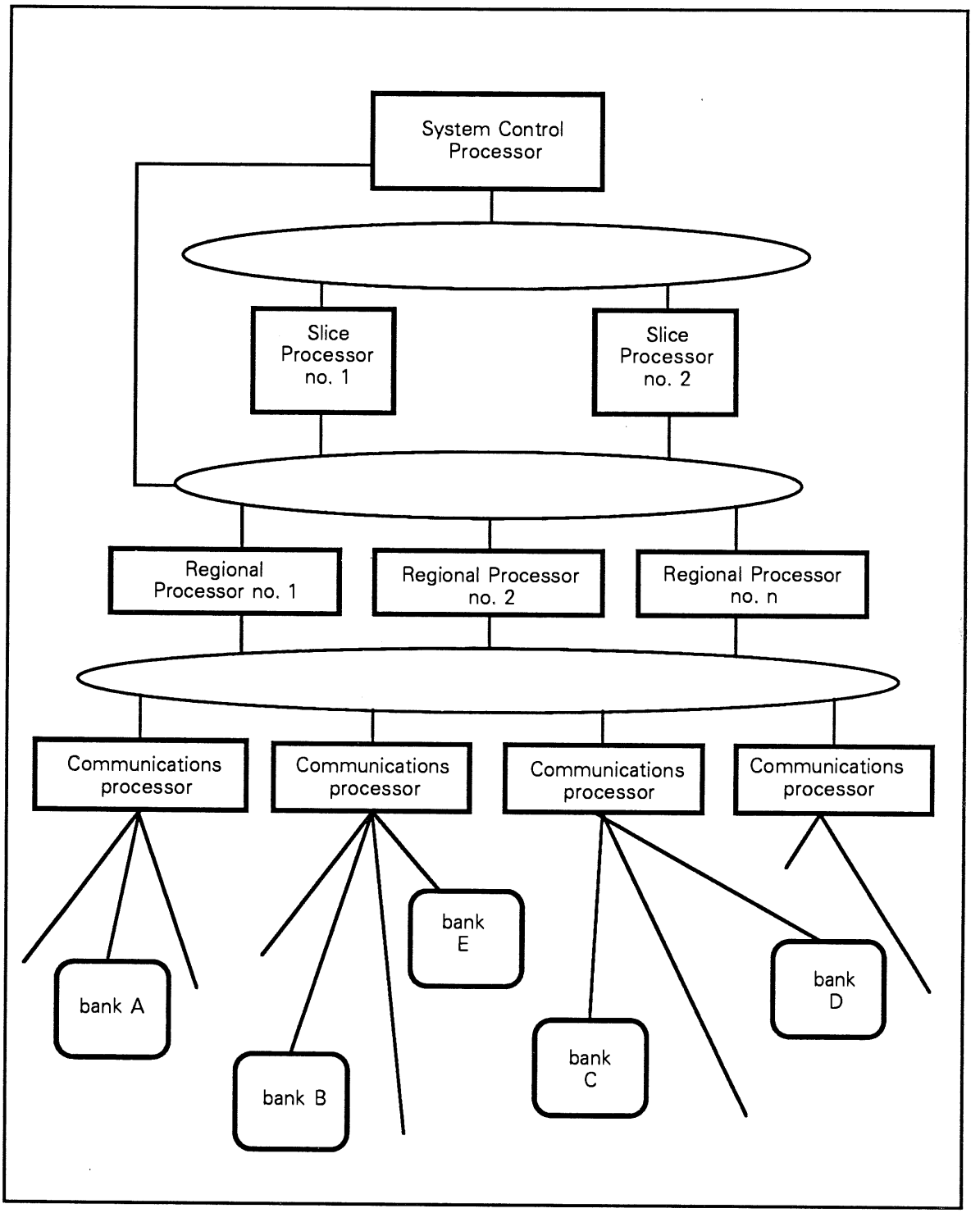
SWIFT is te beschouwen als een toepassing van Electronic Data Interchange (EDI). Dit is een (verzamel)naam voor omgevingen waarbij sprake is van elektronische uitwisseling van gestandaardiseerde berichten tussen twee of meer partijen met behulp van computers en datacommunicatieverbindingen.

Zowel de organisatie als het bestaande netwerk worden aangeduid met de term SWIFT. Het netwerk kan worden gezien als een "value added network", dat door de aangesloten banken voornamelijk wordt gebruikt voor verzending van berichten die betrekking hebben op financiële transacties.

3 Karakteristieken SWIFT

3.1 Netwerkonderdelen

In onderstaand figuur is schematisch weergegeven uit welke hoofdcomponenten het SWIFT-netwerk bestaat.



Deze componenten hebben de volgende functies:
- System Control Processor:
  . monitoring en beheersing van alle netwerkcomponenten en van de toegangsbeveiliging.
- Slice Processor:
  . switchen van Input Regional Processor (IRP) naar Output Regional Processor (ORP) om berichten door te zenden;
  . opslag van berichten (vier maanden on-line);
  . generatie van systeemboodschappen.
- (Input and Output) Regional Processors:
  . input-boodschappenafhandeling;

. boodschappenvalidatie;
. output-boodschappenafhandeling;
. monitoring van afgeleverde berichten.
- Communications Processors:
. aanknopingspunt voor banken;
. stuurt input-berichten door naar de Regional Processor;
. stuurt output-berichten door naar de betreffende bank.
- SWIFT-communicatielijnen (internationale lijnen);
- communicatielijnen naar de banken.

De System Control Processor en de Slice Processor maken deel uit van het System Control Centre. Deze zijn geplaatst in Nederland (Zoeterwoude), België (Brussel) en de U.S.A. (Culpeper). Van de Regional Processors en de Communications Processors zijn er één of meer geplaatst in ieder land.

Communications Processors vormen de intermediair tussen de banken en het SWIFT-netwerk. Een Communications Processor bestaat uit twee delen, namelijk de verbinding met de Regional Processor (onder verantwoordelijkheid van SWIFT) en de verbindingen met de terminals (onder verantwoordelijkheid van de bank).

3.2 Aansluiting op het SWIFT-netwerk

In principe kan elk type computer (dus ook het eventuele mainframe van de bank) gekoppeld worden aan het SWIFT-netwerk. De aan het SWIFT-netwerk gekoppelde computer wordt SWIFT Interface Device (SID) genoemd. Een SWIFT Interface Device wordt ook wel Computer Based Terminal (CBT) genoemd.

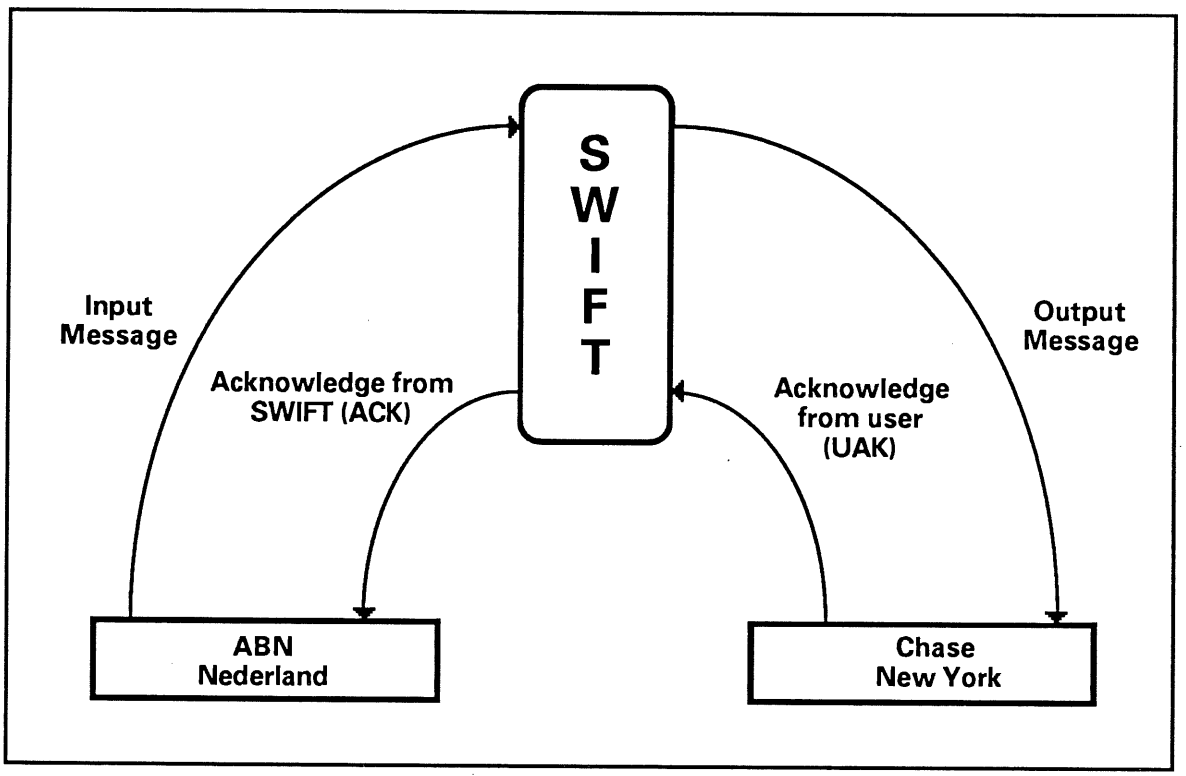
De programmatuur die benodigd is om de computer te laten communiceren met het SWIFT-netwerk kan door de bank zelf worden ontwikkeld, maar zal mede door de SWIFT-organisatie moeten worden geaccepteerd.

SWIFT Terminal Services (STS) is een aparte afdeling van de SWIFT-organisatie welke SWIFT Interface Devices op de markt brengt (zowel de hardware als de software). Deze machines heten SWIFT Terminals en zijn verkrijgbaar in verschillende typen. De hardware kan ook door een aantal andere leveranciers worden geleverd. In dit geval wordt de software wel geleverd door SWIFT.

Er kunnen meerdere gebruikers worden gedefinieerd op een SWIFT Terminal. Aan deze gebruikers kunnen bevoegdheden worden toegekend met betrekking tot bijvoorbeeld het invoeren, verifiëren en autoriseren van berichten.

3.3 Verantwoordelijke instanties

Schematisch kan het verzenden van een bericht van bijvoorbeeld de ABN in Nederland naar de Chase Manhattan Bank in Amerika als volgt worden voorgesteld.



De ABN verzendt een bericht naar SWIFT. Indien het bericht goed wordt ontvangen, stuurt SWIFT een bericht terug naar de ABN (Acknowledge). SWIFT stuurt vervolgens het bericht door naar Chase. Indien Chase het bericht goed ontvangen heeft, dient Chase hierover een bericht terug te sturen naar SWIFT (User Acknowledge).

Er zijn in dit traject dus drie verantwoordelijke partijen te onderscheiden:
- zendende bank;
- SWIFT;
- ontvangende bank.

Zo is bijvoorbeeld door de SWIFT-organisatie vastgesteld dat van een bank wordt geëist dat zij op werkdagen tussen 08.00 en 18.00 uur minimaal 7 uur in staat is om berichten te onvangen. De verantwoordelijkheden zijn verder gespecificeerd in paragraaf 5.2.4 (afhandeling van systeemberichten).

De verschillende soorten berichten die met behulp van het SWIFT-netwerk kunnen worden verstuurd, worden aangegeven in de bijlage.

3.4 SWIFT-applicaties

SWIFT biedt haar faciliteiten aan de gebruikers aan in de vorm van applicaties. Deze applicaties draaien in het System Control Centre van SWIFT en zijn benaderbaar door hiertoe geautoriseerde gebruikers. Initieel zijn in SWIFT twee applicaties beschikbaar, te weten:

1. de General Purpose Application (GPA). Deze applicatie wordt door de gebruiker benaderd op het moment dat deze inlogt op het SWIFT-netwerk. Eenmaal in deze applicatie kan de gebruiker systeemcommando's genereren en andere applicaties benaderen;
2. Financial Application (FIN). Deze applicatie stelt de gebruiker in de gelegenheid berichten te sturen naar of te ontvangen van andere gebruikers. Een gebruiker benadert de FIN application door middel van het SELECT-commando in de GPA-applicatie.

4 Bedreigingen

In dit hoofdstuk wordt ingegaan op de bedreigingen die kunnen optreden vanaf het moment dat betalingen in de gebruikersorganisatie worden geautoriseerd.

De bedreigingen worden in de volgende vier groepen gerangschikt:
- het wijzigen van berichten na autorisatie;
- het verzenden van ongeautoriseerde berichten;
- het verwijderen van berichten uit de berichtenstroom;
- het lezen en/of analyseren van de berichtenstroom.

De laatste bedreiging is passief: er worden slechts berichten gelezen en eventueel geanalyseerd. De eerste drie bedreigingen zijn actief: er worden berichten toegevoegd, gewijzigd of verwijderd. De bedreigingen kunnen zowel optreden binnen de zendende bankorganisatie als binnen het SWIFT-netwerk. Bij de laatste twee bedreigingen is naar onze mening sprake van een minimaal frauderisico, waardoor aan deze bedreigingen in dit artikel verder geen aandacht wordt besteed.

Het wijzigen van berichten na autorisatie en voor verzending kan geschieden door bijvoorbeeld het wijzigen van het SWIFT-adres (dit is een code aan de hand waarvan SWIFT bepaalt naar welke bank het bericht moet worden verstuurd) en het te betalen bedrag voordat het bericht wordt verzonden. Ook is het mogelijk dat na verzending wordt ingebroken op de datatransmissielijn, en dat het SWIFT-adres en/of het bedrag wordt gewijzigd.

De tweede bedreiging betreft het verzenden en invoegen van berichten die niet zijn geautoriseerd. Hierbij valt te denken aan het genereren en het verzenden van een betaling op een eigen rekening in het buitenland, zonder dat deze betaling door een procuratiehouder is geautoriseerd.

Om de risico's die samenhangen met de genoemde bedreigingen te verminderen, dienen maatregelen van interne controle en beveiliging te zijn getroffen. De mogelijke controlemaatregelen worden beschreven in het volgende hoofdstuk.

5 Maatregelen van interne controle en beveiliging

5.1 Controlefaciliteiten geboden door het SWIFT-netwerk

Om te voorkomen dat misbruik wordt gemaakt van het transportmiddel voor berichten is door de SWIFT-organisatie een aantal voorzieningen getroffen in de vorm van fysieke, organisatorische en programmatechnische maatregelen. In het kader van dit artikel beperken wij ons tot een viertal aspecten waarmee de samenwerkende banken direct te maken hebben. Deze betreffen:
- log-in/log-out-procedure;
- authenticator key-procedure;
- volgnummercontrole;
- undelivered message reporting.

Voorts biedt SWIFT de mogelijkheid van een audit-trail, encryptietechnieken en een automatische error recovery- en herstartprocedure. Hoewel deze aspecten worden geboden door SWIFT, worden ze behandeld onder paragraaf 5.2.

5.1.1 Log-in/log-out- en select-procedure

Periodiek worden door de SWIFT-organisatie log-in-tabellen (op papier) aan de bankorganisaties beschikbaar gesteld. Met behulp van de in deze tabellen vastgelegde codes kan toegang worden verkregen tot het SWIFT-netwerk.

Een entry uit de tabel bestaat uit een log-in sequence number en een log-in key. Deze twee elementen moeten beide worden ingetoetst tijdens de inlogprocedure. Het SWIFT-netwerk houdt bij welk log-in sequence-nummer als laatste is gebruikt en welke dus tijdens de eerstvolgende aanlogpoging gebruikt zou moeten worden. Alleen indien dit nummer én de bijbehorende log-in key juist zijn opgegeven, wordt toegang verkregen tot het netwerk.

De log-in-tabel bestaat uit twee delen, die gescheiden worden verzonden door SWIFT. Het eerste deel bevat de eerste twee karakters van het log-in sequence-nummer en de eerste twee karakters van de bijbehorende log-in key; het tweede deel bevat de laatste twee karakters van het log-in sequence-nummer en de laatste twee karakters van de bijbehorende log-in key. Toegang tot het netwerk kan alleen worden verkregen indien de inhoud van beide delen van de tabel wordt ingevoerd.

Voor de log-in-tabellen wordt onderscheid gemaakt in drie sets van tabellen:
- de "normal log-in table":
  Deze tabel bevat 1200 of 2400 entries, waarmee dus een even zo groot aantal malen kan worden aangelogd;
- de "emergency log-in table":
  Deze tabel bevat 300 entries en kan worden gebruikt wanneer niet op tijd een nieuwe (normale) tabel is ontvangen of deze in het ongerede is geraakt;
- de "fallback log-in table":
  Deze tabel bevat 600 entries, en kan voor bijzondere gevallen (bijvoorbeeld in het geval dat het gebruikelijke System Control Centre uitvalt en naar een andere moet worden uitgeweken) worden gebruikt.

Voor het kunnen uitvoeren van het SELECT-commando (zie paragraaf 3.4) is, vergelijkbaar met het LOGIN-commando, een tabel benodigd met SELECT sequence numbers en de daarbij behorende SELECT-keys. Deze tabel wordt, wederom vergelijkbaar met de LOGIN-tabel, in twee delen door de SWIFT-organisatie verzonden naar de bank. Tevens zijn drie versies van deze tabel beschikbaar:
- de "normal select table";
- de "emergency select table";
- de "fallback select table".

Het gebruik van deze tabellen is vergelijkbaar met de LOGIN-tabellen.

5.1.2 Authenticator key-procedure

Om de rechtmatige herkomst van ontvangen berichten te kunnen vaststellen wordt gebruik gemaakt van de authenticator key-procedure.

De banken dienen onderling (op advies van SWIFT iedere zes maanden) zogenaamde authenticator keys uit te wisselen. Met behulp van deze authenticator key, een door de SWIFT-organisatie beschikbaar gesteld algoritme (dat voor elke bank hetzelfde is) en de volledige inhoud van het bericht, wordt het authenticator-resultaat berekend en aan het bericht toegevoegd (in de trailer).

Bij ontvangst van het bericht dient de ontvangende bank het authenticator-resultaat opnieuw te bepalen. Dat geschiedt met behulp van de uitgewisselde authenticator key en het authenticator algoritme. Dit resultaat moet worden vergeleken met het authenticator-resultaat dat is opgenomen in de trailer van het bericht. Indien de key-resultaten overeenstemmen, is vastgesteld dat de herkomst van het bericht rechtmatig is.

5.1.3 Volgnummercontrole

Om de volledigheid van de berichtenoverdracht tussen een bank en het SWIFT-netwerk te kunnen vaststellen, wordt gebruik gemaakt van een volgnummercontrole.

De bankorganisatie dient haar uitgaande berichten te voorzien van een doorlopende nummering. Met behulp van deze nummering is SWIFT in staat de volledigheid van het (voor SWIFT) aantal ingekomen berichten vast te stellen. Indien wordt geconstateerd dat er nummers ontbreken, dan worden de volgende berichten niet door SWIFT geaccepteerd en wordt hiervan melding gemaakt aan de zendende bank.

Vervolgens kent ook SWIFT aan ieder bericht dat aan een bankorganisatie wordt verzonden een volgnummer toe. Op basis hiervan is de bankorganisatie in staat de volledigheid van het aantal ontvangen berichten vast te stellen.

Op het moment dat een gebruiker een applicatie opstart, wordt voor de duur van die sessie een sessienummer toegekend. De Input Sequence Numbers (ISNs) en Output Sequence Numbers (OSNs) zijn voor applicatie FIN opeenvolgend over alle sessienummers heen; voor de applicatie GPA zijn ze opeenvolgend binnen een sessienummer, voor iedere sessie beginnend bij 0.

De volledigheid van de ontvangen berichten kan voor wat betreft de GPA slechts worden bepaald met het OSN en het betreffende sessienummer. Voor wat betreft de applicatie FIN is slechts het OSN benodigd om deze volledigheid vast te stellen.

In SWIFT II wordt gesproken van een Message Input Reference en een Message Output Reference (MIR en MOR). Zowel het sequence nummer als het sessienummer maken, te zamen met de datum en het SWIFT-adres, deel uit van de MIR of MOR.

5.1.4 Undelivered Message Report

Berichten die, om welke reden dan ook, niet aan de ontvangende bank kunnen worden afgeleverd, worden teruggemeld aan de zendende bankorganisatie met behulp van het Undelivered Message Report (MT082). Het Undelivered Message Report vormt een belangrijk steunpunt van de SWIFT-organisatie voor de controle op de volledigheid van de doorlevering van berichten. In principe wordt elk bericht dat door de SWIFT-organisatie in een schakelcentrum wordt ontvangen tweemaal op magneetschijf vastgelegd, waarna het bericht op bestaanbaarheid wordt gecontroleerd. Indien deze controle een positief resultaat heeft, wordt voor spoedberichten en berichten met prioriteit 12 een bevestiging voor ontvangst aan de zendende bankorganisatie gestuurd (positive acknowledgement). In SWIFT I vindt voor de normale berichten en berichten met prioriteit 11 geen terugmelding aan de zendende bankorganisatie plaats, in SWIFT II zal dat wel het geval zijn.

Vervolgens wordt een derde kopie van het desbetreffende bericht vervaardigd en vindt verdere doorlevering van het bericht plaats. Nadat bevestiging voor ontvangst binnen het SWIFT-netwerk voor aflevering aan de ontvangende bankorganisatie heeft plaatsgevonden, wordt de derde kopie van het bericht verwijderd. Het restant van de derde kopie-exemplaren, waarvan geen aflevering aan de bestemde bankorganisatie heeft kunnen plaats vinden voor de "cut off time", wordt met behulp van het Undelivered Message Report aan de zendende bankorganisatie teruggemeld. Voor spoedberichten vindt de terugmelding plaats op basis van de individuele berichten (MT10 overdue warning, MT11 delivery notification).

5.2 Controlemaatregelen te nemen door de bank zelf

Naast de controlemaatregelen die de SWIFT-organisatie biedt om de risico's met betrekking tot het gebruik van SWIFT te verminderen, dient de bank zelf een stelsel van maatregelen van interne controle en beveiliging te creëren. Dit stelsel dient ervoor om de door SWIFT geboden controlemaatregelen te beheersen en om de risico's die verband houden met omstandigheden binnen de eigen organisatie af te dekken.

5.2.1 Algemeen

Vanaf het ontstaan van transacties tot het verzenden van de hieraan gerelateerde berichten kunnen vele bedreigingen optreden. Om de hiermee samenhangende risico's te verminderen, dient de

organisatie een aantal maatregelen te nemen. Het traject kan worden onderverdeeld in een tweetal deeltrajecten, namelijk het traject van het "aanleverende systeem" en het traject "SWIFT-systeem". In dit artikel wordt verder niet ingegaan op het aanleverende systeem.

In de competentietabel van het SWIFT-systeem is vastgelegd wie berichten kan invoeren, raadplegen, verifiëren en autoriseren. Voorts is vastgelegd wie de authenticator keys in het systeem mag aanpassen en wie re-authentication mag uitvoeren (bij ontvangst van berichten).

In beginsel kunnen de volgende functies worden gescheiden:
- beheer log-in-tabel (gescheiden voor de twee delen);
- invoer van berichten;
- verificatie van berichten;
- autorisatie van berichten (bij ST-terminals valt de autorisatiefunctie samen met de verificatie-functie): voor de autorisatie kunnen twee functionarissen zijn vereist, afhankelijk van het bedrag;
- beheer authenticator keys.

In de meeste situaties zal een dergelijke, ver doorgevoerde functiescheiding niet noodzakelijk zijn. Er zijn drie (samengevoegde) functies nodig om een minimaal niveau van functiescheiding te waarborgen, namelijk:
- beheer log-in-tabel en invoeren van berichten;
- verificatie en autorisatie van berichten;
- beheer van authenticator keys.

Voorwaarde voor de toelaatbaarheid van deze "beperkte" functiescheiding is dat het toekennen van bevoegdheden (dat is het aanbrengen van veranderingen in de competentietabellen van de gebruikers) volledig wordt beheerst. Deze beheersing, alsmede de verantwoordelijkheid met betrekking tot de fysieke beveiliging van het SWIFT-systeem, dient te liggen bij functionarissen, onafhankelijk van de operationele SWIFT-omgeving.

Voor de verificatieprocedure kan:
- worden uitgegaan van de betrouwbaarheid van de aangeleverde transacties in de SWIFT-terminal, waarna de verificatie en/of autorisatie groepsgewijs kan plaatsvinden, of;
- niet worden uitgegaan van de betrouwbaarheid van de aangeleverde transacties in de SWIFT-terminal. In dit geval dienen de transacties individueel te worden geverifieerd aan de hand van overzichten of brondocumenten die zijn geparafeerd door de afdeling die de betalingen heeft geautoriseerd.

5.2.2 Authenticator keys

De authenticator keys worden gebruikt om de ontvangende bank in staat te stellen om te bepalen of het bericht inderdaad van de bank afkomstig is, die als afzender in het bericht staat vermeld. De hoofdbedreiging is dat ongeautoriseerd kennis wordt genomen van deze keys en dat deze worden gebruikt om berichten ongeautoriseerd te verzenden of te wijzigen. De ontvangende bank zal alleen een bericht mogen accepteren indien voor dit bericht het door de ontvangende bank berekende authenticator-resultaat overeenkomt met het resultaat dat met het bericht is meegegeven. Om het risico van ongeautoriseerd key-gebruik te verminderen dienen deze authenticator keys goed te worden beheerd. Deze beheerverantwoordelijkheid dient buiten de operationele SWIFT-omgeving te worden geplaatst. Onder het beheer van deze keys wordt verstaan het genereren van de keys, de uitwisseling van de keys met andere banken, het opslaan van de keys en het updaten van de keys in het SWIFT-systeem.

5.2.3 Log-in/log-out-procedure

Met de log-in-tabellen kan toegang worden verkregen tot het netwerk. Voorkomen dient te worden dat onbevoegden toegang krijgen tot het netwerk en berichten kunnen verzenden. Tijdens de inlog-procedure controleert SWIFT of de bank het juiste log-in sequence number en de daarbij behorende log-in key gebruikt. Indien deze combinatie niet juist is, resulteert dit in een "log-in negative acknowledgement" (LNK). De log-in-procedure zal worden afgebroken.

Zoals reeds vermeld, verzendt SWIFT de twee tabeldelen gescheiden van elkaar. De bank dient er zorg voor te dragen dat de twee tabeldelen ook binnen de bankorganisatie gescheiden blijven. Dit geldt zowel voor de routing als voor het bewaren, zodat ongeautoriseerden niet de beschikking kunnen krijgen over één of beide delen van de tabel. Voorts dienen de tabellen voor noodsituaties gescheiden te worden opgeslagen van de normale tabellen. De fallback-tabel dient bij voorkeur in de back-up-omgeving te worden opgeslagen.

Met de SWIFT-organisatie kunnen afspraken worden gemaakt met betrekking tot de tijden dat gegevensuitwisseling zal plaatsvinden. Buiten deze afgesproken tijden zal SWIFT berichten afkomstig van deze bank niet accepteren.

In het geval dat de verbinding met het SWIFT-netwerk vanuit de SWIFT-organisatie wordt verbroken (automatische log-out) dient de bank acties te ondernemen volgens door de bank opgestelde instructies. Bij de uitvoering van de log-out door het SWIFT-netwerk ten gevolge van een "log-in negative acknowledgement" (LNK), wordt een Log-in-Sequence-Number (LSN) bekend gemaakt dat, te zamen met de daarbij behorende log-in keys, bij de volgende log-in-procedure dient te worden opgegeven.

5.2.4 Afhandeling van systeemberichten

De bank dient controle uit te voeren op de aansluiting van de volgnummers. De resultaten van deze controle moeten worden vastgelegd in een register. Indien nummers ontbreken, dient de bank actie te ondernemen volgens vastgestelde instructies. Berichten kunnen bijvoorbeeld achteraf bij SWIFT worden opgevraagd.

Deze vorm van berichtgeving en -afhandeling stellen de verantwoordelijke instanties (zendende bank/SWIFT/ontvangende bank) in staat hun verantwoordelijkheid te dragen en actie te ondernemen ingeval er in het traject iets fout zou gaan. Deze verantwoordelijkheden zijn als volgt gedefinieerd:

Deze vorm van berichtgeving en -afhandeling stelt de verantwoordelijke instanties (zendende bank/SWIFT/ontvangende bank) in staat hun verantwoordelijkheid te dragen en actie te ondernemen ingeval er in het traject iets fout zou gaan. Deze verantwoordelijkheden zijn als volgt gedefinieerd:

De zendende bank is verantwoordelijk voor het verlies van interest indien:
- geen bevestiging (Ack) is ontvangen;
- het bericht was gemeld op het undelivered message report;
- geen MT011 (MT = Message Type) voor een spoedbericht was ontvangen (before cut-off receiving destination);
- indien geen standaardformaat is gebruikt voor het bericht;
- indien niet direct gereageerd wordt op een indicatie van SWIFT dat er een storing in het SWIFT-netwerk is;
- indien de inhoud van het bericht niet-bestaande SWIFT-adressen bevat.

De SWIFT-organisatie is verantwoordelijk voor het verlies van interest indien:
- de bevestiging voor ontvangst (Ack) door de SWIFT-organisatie is verzonden en de berichten niet op het undelivered message report voorkomen en desondanks toch niet zijn afgeleverd;
- het SWIFT-systeem of personeel faalt;
- de SWIFT-organisatie er niet in slaagt om de bankorganisatie tijdig in te lichten over storing in het SWIFT-netwerk.

De ontvangende bank is verantwoordelijk voor het verlies van interest indien:
- de aan de ontvanger geadresseerde berichten niet tijdig worden verwerkt;
- de ontvangende bank niet direct reageert op systeemberichten met betrekking tot het gebruik van het SWIFT-netwerk;
- geen volledigheid door de ontvangende bankorganisatie wordt vastgesteld van OSN-nummers;

- de ontvanger zich niet houdt aan de "terminal policy" die is beschreven in sectie 3, volume I van het User Handbook;
- de ontvangende bank zich niet houdt aan de "normal banking practice".

Bij de bank dienen procedures aanwezig te zijn met betrekking tot:
- de afhandeling van geweigerde uitgaande berichten;
- toezicht op de bevestigingen van spoedberichten;
- acties op berichten die niet tijdig kunnen worden afgeleverd door SWIFT;
- acties met betrekking tot de ontvangst van berichten met onjuiste authenticator key-resultaten;
- acties tijdens foutsituaties;
- vastleggingen van handelingen en berichten die via het SWIFT-netwerk zijn verwerkt;
- beoordeling van de afhandeling van berichten door een van de dagelijkse verwerking onafhankelijke functionaris.

5.2.5 Audit-trail

Binnen de SWIFT-organisatie is een audit-trail beschikbaar van alle aangeleverde en afgeleverde berichten. Met behulp van Message Input Reference of het Message Output Reference (MIR of MOR) kunnen de berichten van de laatste vier maanden on-line worden opgevraagd door de zender respectievelijk de ontvanger.

Binnen de bankorganisatie wordt in de regel de Message User Reference (MUR), voorheen het Transaction Reference Number (TRN), als kenmerk voor de berichten gehanteerd. De MUR is terug te vinden op de dagafschriften in de administratie van de bank.

De administratie van de bank dient met behulp van een uniek kenmerk (MUR) per transactie op de controleerbare vastlegging van de SWIFT-organisatie te kunnen worden aangesloten. Hierbij kan onderscheid worden gemaakt in:
- journal-bestand voor de verdere verwerking van financiële mutaties binnen de bankorganisatie;
- log-bestand voor het vastleggen van alle handelingen die met het geautomatiseerde systeem worden uitgevoerd en uiteindelijk leiden tot de te verzenden berichten.

5.2.6 Encryption

Om te voorkomen dat berichten tijdens het transport binnen het SWIFT-netwerk ongeautoriseerd worden tussengevoegd of gelezen, maakt SWIFT gebruik van encryptietechnieken. Voor het transport van berichten van de bank naar de SWIFT-organisatie is het de verantwoordelijkheid van de bank om encryptie toe te passen. Hiertoe zal zij zelf encryptie-apparatuur moeten plaatsen. In principe heeft de bank toegang tot de modemkamers van de SWIFT-organisatie voor het aanbrengen en onderhouden van deze apparatuur.

5.2.7 Uitwijkmogelijkheden

Om de continuïteit van het berichtenverkeer via het SWIFT-netwerk te waarborgen, dienen uitwijkmogelijkheden beschikbaar te zijn met betrekking tot:
- lijnverbindingen;
- apparatuur;
- programmatuur;
- SWIFT-netwerk;
- speciale lijsten zoals log-in- en select-tabellen en authenticator keys.

De bank dient deze uitwijkmogelijkheden periodiek te testen. Ten behoeve van externe uitwijk dient een afzonderlijk bestand van authenticator keys te worden onderhouden en dienen de benodigde log-in- en select-tabellen op afzonderlijke locaties te worden bewaard.

5.2.8 Automatische error recovery en herstart

In geval foutdetectie- en herstelroutines zijn opgenomen in het geautomatiseerde proces van gegevensverwerking is het noodzakelijk dat deze routines zijn gedocumenteerd met vermelding van de criteria op grond waarvan de routines worden uitgevoerd.

5.2.9 Verzekering

De te treffen maatregelen van interne controle en beveiliging kunnen nooit volstrekte zekerheid bieden dat geen van de genoemde bedreigingen zal optreden of tot een schade zal leiden. Bovendien kunnen sommige maatregelen te kostbaar zijn in vergelijking met het verwachte schadebedrag. Er kan dan worden overwogen om een verzekering af te sluiten om het restrisico te dekken.

5.2.10 Administratieve afhandeling van transacties

De bank dient achteraf vast te stellen dat alle verzonden en ontvangen transacties juist en volledig in de financiële administratie zijn verwerkt. Hiertoe behoort ook de reconciliatie van de nostro-administratie.

6 Toetsing door accountant en/of EDP auditor

Formeel geredeneerd kan de accountant in het kader van de controle van de jaarrekening voorbijgaan aan de maatregelen van interne controle gericht op de beveiliging van betalings-transacties via SWIFT, zolang maar gewaarborgd is dat de SWIFT-transacties juist en volledig worden verantwoord. Deze waarborg kan ook worden gevonden in maatregelen van interne controle achteraf, bijvoorbeeld de nostro-reconciliatie. Wellicht behoeft de accountant niet eens te steunen op maatregelen van interne controle en kan hij of zij puur gegevensgericht de juistheid en volledigheid van de verantwoording van SWIFT-transacties vaststellen.

Het is echter de vraag of deze formalistische benadering wel is vol te houden, in het licht van de enorme bedragen die met SWIFT-betalingen (kunnen) zijn gemoeid. Een ondeugdelijke organisatie rond het SWIFT-betalingsverkeer kan tot grote schade leiden voor de bank of zelfs tot haar ondergang; het afbreukrisico voor de fungerend externe accountant is navenant groot.

De accountant zal dan ook in het kader van de controle van de jaarrekening aandacht dienen te besteden aan de preventieve beveiligingsmaatregelen rond SWIFT. Navolgend wordt kort ingegaan op de interne controlemaatregelen die in dit opzicht van belang zijn. Ook - of juist - in het kader van een bijzondere opdracht tot het uitvoeren van een onderzoek naar de beveiliging rond SWIFT, dienen deze maatregelen te worden beoordeeld.

De accountant dient te beoordelen of de functiescheidingen ten minste voldoen aan de minimale functiescheiding zoals genoemd in paragraaf 5.2.1 en/of het beheer van de log-in-tabellen en authenticator keys adequaat is geregeld. In de meeste gevallen dient te worden voorkomen dat iemand zowel de beschikking heeft over de log-in-tabellen als de authenticator keys, omdat dan de mogelijkheid bestaat dat bij inbraak in het SWIFT-netwerk berichten worden gewijzigd of ingevoegd. Voorts is niet toegestaan dat één functionaris kan aanloggen, invoeren, verifiëren en autoriseren, omdat dan ongeautoriseerd berichten kunnen worden verzonden. De accountant zal moeten beoordelen of de minimale scheiding in het onderhavige geval voldoende is, of dat er een verdergaande scheiding van functies is gewenst.

Voorts dient de accountant te beoordelen in hoeverre de procedures met betrekking tot de invoer, verificatie, en autorisatie voorkomen dat berichten na autorisatie worden gewijzigd of dat ongeautoriseerd berichten worden verzonden.

De beoordeling dient ook gericht te zijn op de procedures voor het ontvangen en afhandelen van berichten via het SWIFT-netwerk (zie hiervoor paragraaf 5.2.4). Verder dienen procedures aanwezig te zijn om de doorlopende nummervolgorde vast te stellen en met betrekking tot het registreren van alle uitgaande en inkomende berichten en het berekenen van controletotalen over deze berichtenstromen, zodat de bank altijd kan vaststellen dat alle verzonden berichten door SWIFT en de ontvangende bank zijn ontvangen, en dat alle te ontvangen berichten inderdaad zijn ontvangen.

Met encryptietechnieken kunnen verdergaande maatregelen gericht op de betrouwbaarheid en de beveiliging worden geïmplementeerd. Encryptie kan worden gebruikt voor authenticatie en voor geheimhouding. Indien voor de betrouwbaarheid en de beveiliging wordt gesteund op encryptie, dient de accountant de toereikendheid ervan te onderzoeken, waarbij inschakeling van een EDP auditor gewenst is.

Als het continuïteitsaspect eveneens onderdeel uitmaakt van het onderzoek, dient de accountant aandacht te besteden aan de recovery- en restart-procedures, alsmede aan de beschikbaarheid van back-up- en uitwijkvoorzieningen. Deze voorzieningen betreffen de lijnverbindingen, apparatuur, programmatuur en de benodigde tabellen en authenticator keys. Echter, een bank zal voor het versturen van deze berichten altijd terug kunnen vallen op telex- en/of telefax-apparatuur.

De accountant dient de opzet van het stelsel van maatregelen te beoordelen. Voor de toetsing van het bestaan en de werking ervan kan de EDP auditor worden ingeschakeld (met name de softwarematige aspecten). Voorts kan de EDP auditor worden ingeschakeld bij de beoordeling van de betrouwbaarheid van de geautomatiseerde aanleverende systemen en van de (eventuele) geautomatiseerde koppeling tussen het aanleverende systeem en het SWIFT-systeem.

Indien sprake is van koppeling van het centrale computersysteem van de bank aan het SWIFT-netwerk rechtstreeks of via een SWIFT-terminal, zal moeten worden onderzocht in hoeverre dit centrale systeem onderdeel dient uit te maken van het onderzoek.

De beslissing hieromtrent heeft veelal te maken met het moment waarop feitelijke autorisatie van het bericht plaatsvindt en de wijze waarop dit gebeurt.

7 Migratie van SWIFT I naar SWIFT II

Het SWIFT I-netwerk is ontworpen en geïmplementeerd in de eerste helft van de jaren zeventig. Met de toename van het berichtenverkeer (meer berichten per bank en meer aangesloten banken) wordt de capaciteit de laatste jaren nagenoeg ten volle benut en is uitbreiding benodigd.

Om hieraan te kunnen voldoen is het SWIFT II-netwerk ontworpen dat zich, afgezien van de grotere capaciteit, onderscheidt van het SWIFT I-netwerk door een andere structuur. Deze verschillen zijn echter niet zodanig dat diepgaande organisatorische en procedurele veranderingen bij de banken zijn vereist.

De migratie naar het SWIFT II-netwerk zal - na een migratietest waaraan een groot aantal banken uit 6 landen (inclusief Nederland) meewerkt - in 1990 van start gaan en ongeveer 2,5 jaar gaan duren.

BIJLAGE

Soorten SWIFT-berichten

1 Customer Transfers
- 100 Customer Transfers
- * Cheque Transactions
- 19n Common Group

2 Bank Transfers
- 20n Bank Transfers
- 21n Advice to Receive
- 29n Common Group

3 Foreign Exchange
- 30n Foreign Exchange
- 32n Fixed Loan/Deposit
- 33n Call/Notice Loan/Deposit
- 35n Advice of Interest Payment Transactions
- 39n Common Group

4 Collections
- 40n Advice of Payment
- 41n Acknowledgements
- 42n Tracers
- 43n Amendments
- 49n Common Group

5 Securities
- * Buying/Selling of Shares/Bonds
- * Coupons
- * Dividends
- 580 Cedel
- 59n Common Group
- 599 Free format

7 Documentary Credits
- * Currently under development. The Free Format message is available as an interim measure.
- 799 Free Format

8 Special payment mechanisms
- * Bank Card message types are currently under Development. The Bank Card (Interim) and Free Format messages are available as an interim measure.
- 88n Bank Cards (Interim)
- 899 Free Format

9 Special Messages
- 90n Confirmation of Debit
- 91n Confirmation of Credit
- 95n Statements
- * Safety/Warning Messages
- 99n Common Group

* nog niet gespecificeerde berichten (in ontwikkeling)

PERSONAL PROFILES

Ir. S.L. Lelieveldt
Studeerde bedrijfskunde aan de Universiteit Twente.
In het kader van zijn afstudeeropdracht voerde hij een inventariserend onderzoek uit naar normalisatie en standaardisatie op het gebied van elektronisch betalingsverkeer. Over dit afstudeeronderzoek, dat plaatsvond als vervolg op een stage bij KPMG Klynveld EDP Audit in Amsterdam, is in februari 1989 een verslag in boekvorm verschenen onder de titel "Elektronisch betalen goed geregeld?".

M. Groesz
Is sedert mei 1985 in dienst bij KPMG Klynveld EDP Audit. Als junior EDP auditor houdt hij zich sinds 1988 in het bijzonder bezig met de ontwikkelingen op het gebied van electronic data interchange.

Drs. A. Hemelaar RA
De heer drs. A. Hemelaar RA is thans adjunct-directeur Interne Accountantscontrole & Beveiliging bij de BankGiroCentrale. Tot voor enige jaren leidde hij de afdeling Beleidsvoorbereiding en Research bij deze onderneming. Uit hoofde van deze functies kan hij worden gezien als een specialist op zowel het gebied van het betalingsverkeer als dat van logische beveiliging.

Drs. H.C. Kocks RA
Vennoot van KPMG Klynveld EDP Audit met een brede ervaring op diverse terreinen van EDP-auditing. Verder is hij regelmatig spreker op seminars over onderwerpen betreffende de EDP-auditing. Hij is tevens universitair docent aan de Erasmus Universiteit te Rotterdam. Van zijn hand zijn diverse publikaties verschenen over het vakgebied.

Drs. T.P. de Vries
De heer drs. T.P. de Vries is eind 1986 bij KPMG Klynveld EDP Audit in dienst getreden.
Hiervoor studeerde hij wiskunde aan de Universiteit van Amsterdam. In het kader van zijn bijvak verdiepte hij zich in mathematische en dynamische beslissingsproblemen.
De heer De Vries heeft zich gespecialiseerd in de beveiligingsmethoden voor het Elektronisch berichtenverkeer, smartcard- en magneetstripkaarttoepassingen en de onderliggende mathematische en cryptografische principes. Hiernaast is hij project-manager Mathematische ondersteuning.
Hij is betrokken bij onderzoeken naar de betrouwbaarheid van het key management en de cryptografische aspecten van elektronische betaalsystemen. Het betreft opdrachten bij financiële instellingen, creditcard-maatschappijen en de detailhandel.
De heer De Vries heeft in januari 1990 zijn postdoctorale studie EDP audit aan de Katholieke Universiteit Brabant afgerond.

Ing. G.H.M. Meijer
Is sinds 1985 werkzaam bij KPMG Klynveld EDP Audit. Hij heeft in 1989 zijn AMBI-opleiding voltooid en studeert momenteel postdoctorale EDP Auditing aan de Erasmus Universiteit te Rotterdam. Hij heeft EDP-audits uitgevoerd op het gebied van rekencentra, besturingssystemen, beveiligingspakketten en SWIFT.

A.H. Kuijlaars RA
Opleiding voor beroepsofficier bij de Koninklijke Militaire Academie te Breda. In 1974 afgestudeerd als Registeraccountant na een 3-jarige stageperiode bij Frese Hogeweg respectievelijk Klynveld Kraayenhof & Co.
In 1976/1977 de opleiding EDP-auditing gevolgd bij KPMG. Tot medio 1986 werkzaam geweest bij het ministerie van Defensie in diverse accountants- en management-functies. Sedert juli 1986 hoofd Interne Accountantsdienst van Postbank N.V.

Drs. C.P. Aland RA
Hoofd IAD/EDP-audit van de Postbank sinds 1 december 1986. Vervulde eerder soortgelijke functies

bij een verzekeringsbedrijf en een industriële onderneming. Is sinds 1975 werkzaam op het terrein van de EDP-auditing en daarvoor gedurende 7 jaar in diverse functies in de automatisering.

Drs. P.M. Knuvers
Studeerde bedrijfseconomie aan de Katholieke Universiteit Brabant met als afstudeerrichting Systeem- en Programma-ontwikkeling. Hij volgt nu de postdoctorale studie accountancy, en is hiermee gevorderd tot controleleer. Is sinds 1987 werkzaam bij KPMG Klynveld EDP Audit, momenteel als junior EDP auditor. Behalve onderwerpen uit de algemene EDP Audit-praktijk (zoals systeembeoordelingen en rekencentrumonderzoeken) heeft het bankwezen zijn bijzondere interesse, met name gericht op internationale geautomatiseerde banksystemen.

RECENTE ONTWIKKELINGEN OP HET TERREIN VAN DE INFORMATIONELE PRIVACY

door mr. V.A. de Pous

Op 1 juli van het vorige jaar is de Wet Persoonsregistratie voor een groot deel in werking getreden. Op 1 januari 1990 is het tweede deel van de wet ingevoerd. De wet regelt het verzamelen en gebruik van persoonsgegevens in geautomatiseerde en manuele registraties. De wet kent een aantal materiële normen, en hanteert daarbij een systeem van gelede normstelling. Wettelijke privacy-normen worden dus nader geconcretiseerd in een aantal algemene maatregelen van bestuur. Een belangrijke nadere regeling betreft het Besluit genormeerde vrijstelling, die op standaardregistraties van toepassing is. Deze en andere recente ontwikkelingen in het kader van de informationele privacy zet mr. V.A. de Pous voor Compact op een rij.

Ter introductie

Hoewel bijna twintig jaar geleden in Nederland voor het eerst belangstelling ontstond voor de bescherming van de persoonlijke levenssfeer in relatie tot persoonsgegevens, zijn vooral de afgelopen vijf jaar pas interessant geweest. Belangwekkende jurisprudentie, gezaghebbende publikaties en het moeizame wetgevingsproces van het tweede ontwerp privacy-wet gaven langzamerhand invulling aan de rechten en verplichtingen van houder, bewerker en geregistreerde. Maar met de Wet Persoonsregistratie (WPR; Wet van 28 december 1988; Staatsblad 1989, 665) in werking zijn wij er nog niet. Niet alleen moeten nog enkele algemene maatregelen van bestuur in werking treden, ook zullen Registratiekamer en rechter normen in het concrete geval moeten aanscherpen. Om eens twee hete hangijzers te noemen: Wat houdt de wettelijke beveiligingsplicht van de houder nu precies in? En: welke handmatige bestanden van persoonsgegevens vallen onder de reikwijdte van de wet?

De inwerkingtreding van de WPR vindt gefaseerd plaats. De eerste fase is op 1 juli 1989 aangevangen. Persoonsregistraties mogen vanaf die datum alleen maar voor een - duidelijk omschreven - redelijk doel zijn aangelegd, de houder ervan zal moeten instaan voor de juistheid en volledigheid van de opgenomen persoonsgegevens en er zullen allerlei technische en organisatorische beveiligingsmaatregelen moeten worden getroffen. Ook heeft de geregistreerde dan eindelijk zijn wettelijk inzage- en correctierecht, terwijl zijn gegevens niet zomaar aan anderen mogen worden verstrekt.

Daarna volgde fase 2 op 1 januari 1990. Overheid, onderwijs, gezondsheidszorg en maatschappelijke dienstverlening enerzijds en bedrijfsleven anderzijds moeten vanaf begin van dit jaar voor **nieuwe** persoonsregistraties aan hun reglement- en formulierplicht gaan voldoen en de verzamelingen van persoonsregistraties aanmelden bij de in Rijswijk gevestigde Registratiekamer.

Reeds **bestaande** registraties moeten voor 1 juli 1990 worden aangemeld.

Voor de aanmelding is een officieel aanmeldingsformulier vastgesteld door de minister van Justitie.

De derde fase van de WPR bestaat in de algemene maatregel van bestuur voor "gevoelige gegevens", die uiterlijk op 1 juli 1990 in werking moet treden. De tekst van deze regeling is nog niet bekend.

Besluit genormeerde vrijstelling

Houders van standaardregistraties zijn vrijgesteld van de verplichting om een privacy-formulier en -reglement te hebben, waarin de registratie omschreven staat. Ook behoeven deze veelal eenvoudige registraties niet bij de Registratiekamer te worden aangemeld. Wel blijven inzage- en correctierecht en andere voorschriften van de WPR van toepassing, waaronder de beveiligingsplicht van de houder voor zijn bestanden. Men noemt dit de genormeerde vrijstelling.

De WPR kent een nogal complex systeem van uitzonderingen, hoewel de hoofdregel simpel is. Iedere registratie met persoonsgegevens valt onder de wet. Echter sommige overheidsbestanden hebben niets met de WPR van doen, omdat daarvoor reeds bijzondere regelgeving gemaakt is of nog gemaakt moet worden. Op andere verzamelingen van persoonsgegevens is slechts een deel van de nieuwe wet van toepassing, terwijl weer andere bestanden conform alle voorschriften van de privacy-wet moeten worden behandeld.

Tot de wettelijke uitzonderingen die in het geheel niet onder de werking van de privacy-wet vallen behoren persoonsregistraties voor persoonlijk of huishoudelijk gebruik zoals zakagenda en dergelijke, bestanden die uitsluitend ten dienste staan van de media en registers die bij of krachtens wetten zijn ingesteld (onder andere Wet op de inlichtingen- en veiligheidsdiensten, Politiewet). De uitzonderingen worden momenteel bij algemene maatregel van bestuur verder uitgebreid. "Hierbij gaat het om persoonsregistraties waarvan het tot dusverre geldende wettelijke regiem strijdig of onverenigbaar is met de nieuwe wet", aldus de Memorie van Toelichting. De aangewezen overheidsbestanden, waarop de WPR eveneens niet van toepassing is, zijn:
1. verschillende justitiële registers;
2. het testamentenregister;
3. bevolkings- en verblijfregisters;
4. het centrale register inschrijving studenten;
5. het kentekenregister;
6. het register inzake vestigingsvergunningen en -ontheffingen.

Dit besluit geldt voor een termijn van drie jaar en kan bij wet worden verlengd.

Bij het Besluit genormeerde vrijstelling, dat op 10 januari 1990 in werking is getreden, heeft de wetgever voor ogen gehad dat gegevensbestanden waarvan duidelijk is dat ze bestaan, geen nadere beschrijving in de vorm van een formulier (particuliere sector) of reglement (overheidssector) behoeven.

In het Besluit genormeerde vrijstelling worden respectievelijk genoemd:
1. administraties van leden of begunstigers in het algemeen en van kerkgenootschappen en andere genootschappen op geestelijke grondslag in het bijzonder;
2. personeelsadministraties, salarisadministraties, administraties betreffende aanspraken op uitkeringen in verband met de beëindiging van een dienstverband, pensioen of vervroegde uittreding;
3. administraties van afnemers en leveranciers, administraties van oud-leden en dergelijke;
4. combinaties van deze administraties;
5. persoonsregistraties gehouden door een derde, betreffende administraties;
6. personen aan wie een vergunning en dergelijke is verleend of die aan een meldingsplicht hebben te voldoen;
7. persoonsregistraties met een archiefbestemming;
8. persoonsregistraties gehouden door instellingen of diensten voor wetenschappelijk onderzoek of statistiek en
9. persoonsregistraties ten dienste van het interne beheer van de organsiatie van de houder, persoonsregistraties met voor communicatie bestemde gegevens.

Inzagerecht mag maximaal 10 gulden kosten

Wat al door de rechter was vastgesteld, heeft inmiddels een wettelijke basis. Sinds 1 juli 1989 is de geregistreerde op grond van de Wet Persoonsregistratie bevoegd om inzage in en eventueel correctie van zijn persoonsgegevens te verlangen. Oefent hij zijn rechten ter zake uit, dan mag de houder op zijn beurt hiervoor ten hoogste *f* 10 in rekening brengen.
Waarom deze regeling, die in een algemene maatregel van bestuur is vastgelegd? De vorige minister van Justitie legde het als volgt uit. Enerzijds is het niet billijk dat de kosten die met inzage gepaard gaan, geheel ten laste van de houder komen. Anderzijds is maximalisering gewenst om belemmering van het inzagerecht te voorkomen.

De maatregel geeft tevens aan dat de inzage- en correctieverplichtingen van de houder **geen** prestaties zijn in de zin van de Wet op de omzetbelasting 1968. Over de door de verzoeker betaalde vergoeding is dus geen BTW verschuldigd.

Mag dan de consumentenorganisatie Stichting Waakzaamheid Persoonsregistratie een modelbrief voor inzage hebben opgesteld, het is nog maar de vraag of een en ander schriftelijk kan worden afgehandeld. Gelet op de verplichtingen die de wet de houder oplegt, zoals het in beginsel niet verstrekken van persoonsgegevens aan derden en de beveiliging van de bestanden, zal de verzoeker zich dienen te legitimeren.

In het geval de houder inzage weigert of wanneer hij op verzoek van de betrokkene of op bevel van de rechter tot verbetering, aanvulling of verwijdering is overgegaan, moet de houder overigens de betaalde kostenvergoeding teruggeven aan de geregistreerde.

De Registratiekamer

Op grond van de WPR is er een nieuw, onafhankelijk bestuursorgaan ingesteld, de Registratiekamer, die belast is met het toezicht op de naleving van de wet. De kamer heeft een groot aantal - veelal moeilijke - taken van de wetgever meegekregen. Zo is de kamer allereerst een adviesorgaan van de regering met betrekking tot alle wetgeving en het te voeren beleid op het terrein van de informationele privacy-bescherming. Daarnaast heeft de wetgever de kamer ook een adviesfunctie ten opzichte van de rechter gegeven. Dan is er de (repressieve) toezicht- en controlerende functie op de naleving van de privacy-voorschriften, terwijl de Registratiekamer tegelijkertijd als de instelling voor de behandeling van klachten moet worden beschouwd.

Ook heeft het bestuursorgaan een toetsende functie gekregen en wel met betrekking tot de branche-gewijze zelfregulering (de gedragscodes) en zal het overigens tevens een belangrijke bijdrage gaan leveren aan de concretisering van de normstelling op dat terrein. Vervolgens heeft de kamer een registratieve functie wat betreft de aanmelding van persoonsregistraties. Verder zijn er nog verschillende Europeesrechtelijke taken. De kamer bestaat uit een voorzitter, twee leden, verschillende plaatsvervangende leden en een secretariaat ter ondersteuning.

Volgens voorzitter mr. K. de Vries zijn een aantal zaken essentieel voor het functioneren van de Registratiekamer. Een ervan is de onafhankelijkheid van het bestuursorgaan. Waar liggen op dit moment de prioriteiten van de kamer? Allereerst wil de kamer zoveel mogelijk geschillen langs de weg van bemiddeling tot een daadwerkelijke oplossing brengen, zodat de stap naar de rechter zo veel mogelijk wordt voorkomen. Daarnaast zal de kamer mede aan de hand van de verplichte meldingen, die vanaf 1 januari in 1990 binnen zullen komen, het veld van persoonsregistraties systematisch in kaart brengen. Door de ontwikkeling nauwlettend te volgen zal dan worden bekeken waar de beschikbare mankracht zo effectief mogelijk kan worden ingezet.

Voor wat betreft de adviestaak van de kamer, zowel ten opzichte van de regering als de rechter, acht de voorzitter het noodzakelijk dat de Registratiekamer zich in zeer korte tijd ontwikkelt tot een expertisecentrum.

Nadere informatie:
Ministerie van Justitie. Sinds 1 juni 1989 is de WPR-informatietelefoon van het ministerie van Justitie operationeel: 070 - 56.33.95. Geheel nieuw is het WPR-loket, dat via bladzijde *67813# in Viditel 24 uur per dag toegankelijk is. Dit systeem biedt verschillende faciliteiten en rechtzoekenden kunnen tevens vragen stellen.

Registratiekamer. Het nieuwe, onafhankelijke bestuursorgaan - de Registratiekamer - is bereikbaar onder telefoonnummer 070 - 3190.190. (telefax: 070- 940.460) Bezoekadres: Gebouw Hoogvoorde, Sir Winston Churchilllaan 362 in Rijswijk. (Postadres: Postbus 3011, 2280 GA Rijswijk.)

Bij de Registratiekamer kan schriftelijk het officiële aanmeldingsformulier voor persoonsregistraties worden aangevraagd.

OVERZICHT HOOFDARTIKELEN 1987/1989

Een selectie van geactualiseerde artikelen uit de 12,5 jaar Compact (1974 - 1986) is opgenomen in het boek "24 over EDP-auditing". 24 Auteurs over EDP-auditing in theorie en praktijk: visies, ontwikkelingen, werkwijzen en oplossingen.
Het boek is verkrijgbaar via de boekhandel onder nummer: ISBN 90 14 03648 5.

43	14e jaargang 87/1 winter 86/lente 87	
	- Internationaal literatuuronderzoek naar computermisbruik in strafrechtelijk perspectief	mr. V.A. de Pous
	- Geïntegreerde gegevensverwerking	drs. H.C. Kocks RA
44	14e jaargang 87/2 zomer 1987	
	- Consequenties voor de beheersbaarheid ten gevolge van nieuwe technologische ontwikkelingen	A.W. Neisingh RA
	- Betalingsorganisatie en automatisering binnen de organisatie	J. ten Wolde RA
	- Electronic Banking-systemen in de praktijk	drs. D.M. Swagerman
45	14e jaargang 87/3 herfst 1987	
	- Escrow-depot voor computersoftware in Nederland	mr. V.A. de Pous
	- Beveiligen tegen computermisbruik	A.W. Neisingh RA en drs. J. Vossen
	- Geïntegreerde gegevensverwerking: Structuur van controle- en beveiligingsmaatregelen in een ADR/DATACOM DB-DC-omgeving	J.A.W. Winterink RA en drs. R.G.A. Fijneman
	- Belangrijke functies van een toegangsbeveiligingspakket	M.C. Duym
46	14e jaargang 88/1 winter 1987/1988	
	- SKE, Structured Knowledge Engineering	ing. A. van der Vlist
	- Beveiliging bij datatransmissie	ing. H.A.J.M. Spape
	- Electronic Funds Transfer, het elektronisch uitvoeren van betalingen (literatuurstudie)	mw. ing. I.M. van Duin
47	15e jaargang 88/2 lente/zomer 1987	
	Special van de sectie Software Engineering	
	- De sectie Software Engineering, een inleiding	H. Veenman
	- Software Engineering	H. Veenman en ing. L.J.M.W. Gielen
	- Het testen van software	O. Kluyt
	- UNIX	ing. A. van der Vlist en ing. J.C. van Winkel RI
	- Computervirussen	ing. J.C. van Winkel RI
	- Objects	ing. L.J.M.W. Gielen
	- HyperCard	J. Schalk
	- Programmeertheorie	J. Schalk
	- Het Apple Talk netwerk, een beschouwing	J.L. Ramos Najera
	- PS/2 - OS/2	ir. J. de Graaff en drs. D.J.P. Witte
	- Elektronisch betalen, de betaalpas	ing. J. Rotteveel
48	16e jaargang 89/1 lente 1989	
	- Het uitvoeren van een transactie-analyse	M.C. Duym
	- Software escrow	R.A. s'Jacob
	- Computervirussen. Worm in groot netwerk	drs.ing. J.C. van Winkel RI
	- Beheersaspecten bij gebruik van microcomputers	J.F.C. van Epen CISA
	- The IBM AS/400. A concern to the EDP Auditor?	H.J. Lijnes

	- AS/400 security	mw. V. Six
	- Internationale gegevensstromen: abstract en moeilijk te controleren	mr. V.A. de Pous
49	16e jaargang 89/2 zomer 1989	
	- Beveiliging, noodzaak?	J.L.H. Kooijman RA
	- Beveiligingsbeleid formuleren	drs. R. Schenk
	- Informatiebeveiliging in het kader van automatisering	drs. H.C. Kocks RA drs.ing. H.A.J.M. Spape RA
	- De keuze van beveiligingsmaatregelen in een geautomatiseerde omgeving	drs. J. Kuipers RA
	- De praktische methode voor de analyse van risico's bij automatisering	ing. C.J.M. Gielen
	- Organisatorische beveiliging van de geautomatiseerde gegevensverwerking	J.C. Boer RA
	- Fysieke beveiliging	J.F.C. van Epen CISA
	- Beveiligingsaspecten van computernetwerken	drs.ing. H.A.J.M. Spape RA
	- Logische toegangsbeveiliging	J. Brinkman
	- Beveiliging van de informatie in geautomatiseerde personeelsregistratiesystemen	J.F.C. van Epen CISA