COMPACT WINTER

ELEKTRONISCH BETALINGSVERKEER

1992/4

KWARTAALBLAD EDP-AUDITING

Compact ®
Jaargang 19, nummer 4
Een uitgave van KPMG Klynveld EDP Auditors en Samsom BedrijfsInformatie, werkmaatschappij van Wolters Kluwer NV.
Het blad verschijnt 4 x per jaar.

Redactie
D. Steeman RE RA (hoofdredacteur)
drs. R.G.A. Fijneman RE RA
prof. A.W. Neisingh RE RA
drs. P. Veltman RE RA

Redactiesecretariaat
Mw. A.M.F. Hofland,
KPMG Klynveld EDP Auditors,
K.P. van der Mandelelaan 41,
3062 MB Rotterdam
Tel.: 010 - 453 47 40
Fax : 010 - 453 47 77

Vormgeving
Bureau Karakter, Delft

Aan dit nummer werkten mee
mr. R.E. van Esch /
E.R. Fekkes /
drs. F.G. Knaack /
mw. drs. M.C. van Lith /
drs. R. Oudega /
H. Roos RA /
ir. G.J. Schuringa /
H.Veenman MBT

Abonnementen
f 135,- per jaar incl. BTW. Losse nummers f 45,- incl. BTW. Abonnementen kunnen schriftelijk tot uiterlijk één maand voor de aanvang van een nieuw abonnementsjaar worden opgezegd. Bij niet tijdige opzegging wordt het abonnement automatisch met een jaar verlengd.

Abonnementsadministratie
Samsom BedrijfsInformatie,
Postbus 4,
2400 MA Alphen aan den Rijn
Tel.: 01720 - 6 68 00
Fax : 01720 - 7 59 33
Adreswijzigingen - ook tijdelijke - moeten minstens 8 weken voor de verschijningsdatum bekend zijn.

Uitgever
J.R.M. Masselink

Lid van de Nederlandse organisatie van tijdschriftuitgevers NOTU

ISSN 0920 - 1645

INHOUDSOPGAVE

REDACTIONEEL

Het blad wil een bijdrage leveren aan de ontwikkeling van het vakgebied EDP-auditing door het publiceren van actuele artikelen op deelterreinen van EDP-auditing en advies, zoals: • beoordeling automatiseringsorganisaties en -systemen • risicobeheersing • telecommunicatie-adviezen • beveiligingsonderzoeken • quality assurance • opleidingen en trainingen • privacy-wetgeving • computercriminaliteit en nieuwe regelgeving. Behalve voor EDP-auditors kan dit blad ook interessant zijn voor EDP-deskundigen en gebruikers van informatiesystemen. De in dit tijdschrift weergegeven meningen mogen niet worden gezien als officiële zienswijze van KPMG Klynveld EDP Auditors.

Het blad Compact is met de meeste zorg samengesteld. Niettemin is het niet geheel uitgesloten dat de geboden informatie enkel en alleen door tijdsverloop en/of andere oorzaken minder juist is. Noch KPMG Klynveld, KPMG Klynveld EDP Auditors, noch de redacteuren persoonlijk, noch uitgeverij Samsom BedrijfsInformatie BV, deel uitmakend van Wolters Kluwer NV, aanvaarden enige aansprakelijkheid, hoe ook genaamd, uit welken hoofde dan ook voor enig gevolg rechtstreeks of indirect voortvloeiend uit het gebruik van de informatie.

De redactie stelt gaarne ruimte in Compact beschikbaar voor reacties en/of ervaringen van lezers. Auteurs die overwegen een bijdrage te leveren, wordt verzocht kennis te nemen van de aanwijzing voor auteurs, die bij het secretariaat verkrijgbaar is.

Vanaf de jaren vijftig heeft in Nederland het girale betalingsverkeer een hoge vlucht genomen. Het gebruik van girale betaalrekeningen bood tal van voordelen: voor de banken goedkope financiering en de mogelijkheid andere bankprodukten af te zetten en voor de particuliere en zakelijke cliënt gemak, veiligheid en kostenbesparing.

Dit goed ontwikkelde girale betalingssysteem, in combinatie met de hieraan gekoppelde gegarandeerde betaalmiddelen, heeft lange tijd de introductie van nieuwe betaalinstrumenten in de weg gestaan. In dit opzicht is sprake van de werking van de wet van de remmende voorsprong. De laatste jaren echter laten op het gebied van het betalingsverkeer in Nederland een turbulente ontwikkeling zien.
Betalingsverkeer is voor de banken een kernactiviteit geworden, in plaats van een nevendienst die ondergeschikt is aan het overige bankbedrijf. Deze wijziging van strategie bracht een verhoogde aandacht voor de rentabiliteit van deze activiteit met zich mee. Tegenover de kosten, vooral automatiseringskosten, staan baten uit hoofde van rentemarge, valutering en omzetprovisie. Uit een onderzoek dat KPMG in 1990 uitvoerde naar de rentabiliteit van het betalingsverkeer kwam naar voren dat dit in het peiljaar 1989 praktisch kostendekkend was, maar dat over de jaren 1987 en 1988 een verlies werd geleden van ruim f 2,5 miljard.

Bovenstaande ontwikkeling betekent een stimulans voor de invoering van efficiëntere betaalmiddelen, waarbij te verwachten is dat een verdere substitutie zal plaatsvinden van papieren informatiedragers door datacommunicatie. Door onder andere tarifering kan een sturing worden bewerkstelligd in de richting van elektronisch betalen, zowel bij toonbankbetalingen (met een betaalautomaat) als bij bureaubetalingen (elektronisch bankieren). Elektronisch bankieren is ook voor de (zakelijke) bankcliënt aantrekkelijk door de mogelijkheid van integratie van transactieverwerkende systemen (inclusief EDI-toepassingen) met treasury-systemen.

De beveiliging van elektronische betaalvormen heeft bij de ontwikkeling ervan terecht veel aandacht gekregen. Weliswaar kunnen elektronische betaalinstrumenten als inherent veiliger worden beschouwd dan traditionele betaalvormen, maar mocht zich niettemin een inbreuk op de beveiliging voordoen dan kunnen de hieruit voortvloeiende schade en kosten een enorme omvang aannemen. Zelfs een vermeende inbreuk kan het publieke vertrouwen in deze elektronische betaalvormen ernstig ondermijnen.

Creditcard-betalingen buiten beschouwing gelaten kunnen tot het elektronische betalingsverkeer worden gerekend: elektronisch betalen en elektronisch geld opnemen met een betaalpas, en het elektronisch inzenden van betaal- en incassoopdrachten. Bekende voorbeelden van dit laatste zijn de verschillende electronic banking-produkten die de banken aan de zakelijke en particuliere cliënten ter beschikking stellen, het telegiro (spoed)circuit, alsmede het buitenlands betalingsverkeer via S.W.I.F.T. Hierbij zij opgemerkt dat electronic banking over het algemeen niet alleen de mogelijkheid biedt betalingsopdrachten in te zenden, maar ook functies kent voor cash management (zoals saldo-informatie opvragen en automatische reconciliatie).
In verband met de grote betekenis van datacommunicatie voor deze elektronische betaalvormen is de beveiliging overwegend gebaseerd op cryptografische technieken.

De EDP-auditor kan zowel bij banken als bij bankcliënten in aanraking komen met toepassingen van elektronisch betalen. Om zich een oordeel te kunnen vormen over de toereikendheid van de getroffen beheersmaatregelen gericht op de gestelde of te stellen eisen (zoals eisen van betrouwbaarheid) dient hij/zij inzicht te hebben in de functionaliteit van deze betaalvormen, de aanwezige risico's en de mogelijke oplossingen.
De redactie verwacht dat deze uitgave van Compact hieraan een bijdrage kan leveren.

Drs. P. Veltman RE RA

De veiligheid van betaalautomaten

E.R. Fekkes

**Is elektronisch betalen met een betaalpas wel veilig?
De transactiebedragen waar het om gaat zijn betrekkelijk gering, maar daar tegenover staan het grote transactievolume en het grote aantal, fysiek zeer uiteenlopende verkooppunten met betaalautomaat. Een inbreuk op de beveiliging van deze infrastructuur zou dan ook verstrekkende gevolgen hebben.
Fekkes, die als beveiligingsdeskundige werkzaam is bij BeaNet, geeft een schets van de mogelijke inbreuken op de beveiliging van het elektronische betalingsverkeer met een betaalpas en van de daartegen getroffen maatregelen.**

INLEIDING

Elektronisch betalen en ook de beveiliging hiervan staat sterk in de publieke belangstelling. Het gebruik van deze betaalvorm neemt snel toe. De risico's dienen voor zowel de consument en de detaillist als de bank acceptabel te zijn. Ondanks een veelheid van implementaties dient een hoog beveiligingsniveau te zijn gegarandeerd.

De in het artikel beschreven vorm van elektronisch betalen wordt gehanteerd door het Nederlandse bankwezen. De automaten welke voldoen aan de gestelde eisen, zijn ook inzetbaar voor de afhandeling van andere kaarttypen, zoals creditcards en private label cards.

Door het onderbrengen van alle kritische functies in een specifiek deel van de betaalautomaat (de security box) is het mogelijk de veiligheid van de gehele betaalautomaat te garanderen, indien de veiligheid van alleen de security box is gewaarborgd. Dit kan worden vastgesteld bij een nauwgezette beoordeling. In het algemeen geldt dat de security box een stabiele set van functies kent en derhalve weinig aan software-onderhoud (en daarmee nieuwe beoordeling) onderhevig is.
In dit artikel wordt achtereenvolgens ingegaan op de functionaliteit van betaalautomaten, de risico's, de getroffen beveiligingsmaatregelen en de controle daarop.

De beveiliging van het elektronisch betalen berust voor een belangrijk deel op cryptografische maatregelen. Globaal wordt aangegeven welke technieken worden gebruikt. De achtergrond van deze technieken valt buiten het kader van dit artikel en is derhalve niet verder uitgewerkt.

FUNCTIONALITEIT VAN DE BETAALAUTOMAAT

De betaalautomaat wordt toegepast voor het verrichten van elektronische betalingen op het verkooppunt: Electronic Funds Transfer at the Point Of Sale (EFT/POS). Voor de consument is de werkwijze vergelijkbaar met die van geld opnemen bij de geldautomaat. Voor beide toepassingen wordt gebruik gemaakt van dezelfde pasjes en PIN-code. De werkomgeving van betaalautomaat en geldautomaat is echter sterk verschillend: de geldautomaat is over het algemeen opgesteld in gecontroleerde ruimten (zoals een bankkantoor), terwijl de betaalautomaat op zeer veel verschillende en fysiek uiteenlopende locaties te vinden is. Hierdoor worden aan de betaalautomaat aanvullende eisen ten aanzien van beveiliging gesteld. .
De berichtenuitwisseling tussen betaalautomaat en bank vindt plaats via BeaNet, de centrale schakel voor elektronisch betalen. Hierbij worden door BeaNet de berichten naar automaten en banken op een veilige wijze afgehandeld. De betaalautomaat hoeft hierbij slechts één communicatieprotocol en beveiligingsmethode te kennen. De vertaling naar de specifieke werkwijze van de verschillende banken wordt door BeaNet uitgevoerd. De betaalautomaat maakt in het merendeel van de gevallen voor de verbinding gebruik van de openbare infrastructuur (telefoonnet, Datanet-1).

Afhandeling van de transactie

De betaalautomaat stuurt het transactiebericht naar BeaNet. De transactie wordt door BeaNet gecontroleerd op juistheid, vertaald en voor autorisatie aan de desbetreffende bank aangeboden. Het antwoord van de bank (PIN goed of fout, voldoende saldo) wordt door BeaNet, na weer te zijn gecontroleerd op juistheid, teruggezonden naar de betaalautomaat. Vervolgens stuurt de betaalautomaat een bevestiging van de transactie naar BeaNet. Indien blijkt dat de transactie alsnog niet doorgaat, stelt BeaNet de bank hiervan automatisch op de hoogte. Door BeaNet worden dagelijks de transactiegegevens aangeboden aan de Bank-GiroCentrale voor de verdere verwerking (debitering van de consument en creditering van de winkelier). De transacties van de giromaatpassen worden door de Postbank op het moment van de transactie direct verwerkt.

Vergeleken met de geldautomaat worden aan de betaalautomaat aanvullende eisen ten aanzien van beveiliging gesteld.

Soorten betaalautomaten

Betaalautomaten kunnen in een aantal soorten worden onderverdeeld. De zelfstandige (stand-alone) betaalautomaat voorziet uitsluitend in de afwikkeling van de elektronische betaling. De kassier voert het transactiebedrag in. De klant geeft zijn PIN-code in en accordeert het bedrag. De betaalautomaat verzorgt de afwikkeling van de transactie via BeaNet. Een kassagekoppelde betaalautomaat ontvangt het transactiebedrag automatisch van de kassa. Dit vermindert de door de winkelier te verrichten handelingen en de kans op fouten. Verder gespecialiseerde betaalautomaten worden onder meer in de oliebranche gebruikt. Deze betaalautomaten verzorgen kassafuncties, elektronisch betalen en logistieke functies. Betaalautomaten worden inmiddels ook in self-service-apparaten toegepast.

Aansluitmogelijkheden

Betaalautomaten worden op verschillende manieren aangesloten. In de eenvoudigste oplossing heeft elke betaalautomaat een eigen telefoonaansluiting. Indien hogere transactievolumes worden verwerkt, kan worden gekozen voor Datanet-1 of huurlijnen. In dat geval kunnen meerdere betaalautomaten dezelfde aansluiting gebruiken. Ook een opstelling in een cluster, met toepassing van reeds aanwezige lokale netwerken, is mogelijk.

Transactiesoorten

De standaardafhandeling van een transactie met een bankpas bestaat uit een autorisatieverzoek van de betaalautomaat aan de bank, het antwoord hierop en een bevestigingsbericht. Daarnaast is "pre-autorisatie" mogelijk. Hierbij wordt eerst het beschikbare saldo opgevraagd en het PIN gecontroleerd, waarna de transactie wordt uitgevoerd met als maximumbedrag het opgevraagde saldo. Dit transactietype vindt hoofdzakelijk toepassing bij "buitenpalen" bij benzinestations. Hier wordt dan voor maximaal het genoemde bedrag getankt. Op bepaalde typen betaalautomaten kunnen naast bankpassen ook creditcards worden gebruikt.
De transacties worden in een aantal gevallen volledig lokaal door de betaalautomaat afgehandeld. Ze worden in het geheugen van de betaalautomaat opgeslagen en eens per dag door een centrale computer uitgelezen. Ook online-autorisatie van creditcards wordt door een aantal betaalautomaten ondersteund. Hierbij wordt voor de saldocontrole door de betaalautomaat contact gezocht met de desbetreffende creditcard-maatschappij.

RISICO'S

Het gebruik van betaalautomaten kent een aantal risico's. Sommige daarvan hebben te maken met de juiste afwikkeling van de transactie (zoals het achteraf wijzigen van het bedrag), terwijl andere risico's betrekking hebben op het vervalsen van de

bankpas en het verkrijgen van de PIN-code. Dergelijke vervalste passen kunnen, indien ook de PIN-code bekend is, worden gebruikt in geldautomaten en betaalautomaten.

Gebruiken van valse of gestolen pas

Er dient zekerheid te bestaan over het feit dat de aangeboden bankpas echt is en door de rechtmatige eigenaar wordt gebruikt. De PIN-code zorgt voor de benodigde koppeling: bij elke pas hoort een eigen PIN-code, welke uitsluitend aan de eigenaar bekend wordt gemaakt. De PIN-code is niet op de bankpas aanwezig. De bankpas kent verder een aantal echtheidskenmerken, zoals het Beethoven-hologram op Eurocheque-passen. Ook is in de magneetstrip een aantal gegevens opgenomen die voor derden niet voorspelbaar zijn. Gezien het feit dat de magneetstrip met de juiste apparatuur kan worden gekopieerd, is de geheimhouding van de PIN-code de belangrijkste maatregel om te voorkomen dat een gestolen of vervalste pas door derden wordt gebruikt.

Wijzigen van transactiegegevens

De klant accordeert het door de winkelier ingegeven bedrag. Het bedrag mag hierna noch door de winkelier noch door de klant kunnen worden gewijzigd. Ook de bij de transactie betrokken rekeningnummers dienen tegen wijziging te zijn beschermd. Op deze wijze wordt voorkomen dat een transactie wordt uitgevoerd voor een ander bedrag dan door de klant is geaccordeerd, of wordt overgemaakt van of naar een andere rekening. Verder dient ook het antwoord van de bank op het autorisatieverzoek te worden beschermd. Als dit niet het geval zou zijn, zou de winkelier een positief antwoord naar de klant toe als negatief kunnen doorgeven en om een andere betaling vragen. Zodra de klant dan is vertrokken, wordt de (geautoriseerde) transactie verder afgerond, waardoor de klant twee keer zou hebben betaald.

Genereren valse transacties

Het systeem moet uitsluiten dat transacties worden gegenereerd die niet door een klant zijn uitgevoerd. Ook het meermalen aanbieden van een zelfde transactie (replay) door de winkelier dient onmogelijk te zijn.

Vastleggen van pasgegevens

Zoals reeds eerder is aangegeven, is het kopiëren van magneetstrippassen niet uitgesloten. In de betaalautomaat dienen echter wel maatregelen te worden genomen die de kans op het vergaren van de inhoud van de gebruikte magneetstrippen zo klein mogelijk maken.

Vastleggen van PIN-codes

De veiligheid van de bankpas berust hoofdzakelijk op de geheimhouding van de PIN-code. In de betaalautomaat dient er derhalve voor te worden gezorgd dat het achterhalen van de gebruikte PIN-codes niet mogelijk is.

Uitlezen van sleutelgegevens

Een aantal van de bovengenoemde risico's wordt tegengegaan met behulp van cryptografische maatregelen. De hiertoe benodigde geheime sleutelgegevens dienen niet uit de betaalautomaat te kunnen worden uitgelezen.

Gezien het feit dat de magneetstrip kan worden gekopieerd, is de geheimhouding van de PIN-code de belangrijkste maatregel om te voorkomen dat een gestolen of vervalste pas door derden wordt gebruikt.

Wijzigen van security box-functies

De bescherming van de transactie wordt uitgevoerd in de security box van de betaalautomaat. De hiervoor in de security box aanwezige programmatuur mag derhalve voor derden niet te wijzigen zijn.

BEVEILIGINGSMAATREGELEN

De beveiligingsmaatregelen zijn te verdelen in procedurele maatregelen, cryptografische maatregelen en fysieke maatregelen. In dit artikel worden uitsluitend de maatregelen aan de kant van de betaalautomaat beschreven. Deze maatregelen zijn gericht op de security box. Vergelijkbare maatregelen zijn aanwezig bij de systemen van BeaNet en banken. Met betrekking tot de beveiligingsmaatregelen kan nader onderscheid worden gemaakt naar drie fasen: fabricage, initialisatie en gebruik.

Procedurele maatregelen

Vastgesteld moet worden dat de security box volgens de juiste specificatie is gefabriceerd en geladen is met de juiste programmatuur. Deze authenticiteit wordt bij de fabricage gewaarborgd door het opnemen van een geheime waarde (transportsleutel) in deze box door de fabrikant. Door de fysieke beveiliging van de security box is het niet mogelijk dat derden deze waarde wijzigen of uitlezen of dat de security box wordt geopend of aangepast. De procedures bij de fabrikant dienen te garanderen dat uitsluitend authentieke en correcte

security boxen van de transportsleutel worden voorzien. Deze handeling geschiedt door de afdeling Kwaliteitscontrole van de desbetreffende fabrikant. De fabrikant dient een uitvoerige administratie betreffende de status van de geproduceerde security boxen bij te houden. Ook worden hoge eisen gesteld aan de kwaliteitsbeheersing bij de fabricage.

Initialisatie van security boxen vindt uitsluitend bij BeaNet plaats. Hierbij wordt bij elke box gecontroleerd of de juiste transportsleutel in de security box aanwezig is (authenticiteit) en of de security box is voorzien van de juiste programmatuur (integriteit). Indien deze controle positief uitvalt wordt de box voorzien van de benodigde sleutelgegevens en kan hij door de leverancier aan een betaalautomaat bij een afnemer worden gekoppeld.

Cryptografische maatregelen

Met cryptografische maatregelen wordt bescherming geboden tegen het wijzigen van transactiegegevens en het uitlezen van magneetstripgegevens en PIN-code. Hierbij wordt door de programmatuur in de security box bovendien zorg gedragen voor de juiste volgorde van de afhandeling van de transactie.

De PIN-code wordt na intikken door de klant direct vercijferd en is dus nooit in klare tekst buiten de security box beschikbaar. Het programma van de security box zorgt bovendien ervoor dat de ingegeven PIN-code voor slechts één transactie kan worden gebruikt. De PIN-code wordt vercijferd aan BeaNet verzonden. Bij BeaNet wordt deze door middel van een speciale security box opnieuw vercijferd en naar de desbetreffende bank gezonden. Bij de bank wordt ook weer door middel van een security box gecontroleerd of de PIN-code juist is. De PIN-code is hierbij nergens buiten de genoemde (niet toegankelijke) security boxen in klare tekst aanwezig en derhalve nergens uitleesbaar.

Door de aanwezigheid van een volgnummer in de transactie is het niet mogelijk dezelfde transactie meermalen aan BeaNet aan te bieden.

Het autorisatieverzoek bevat alle voor de transactie benodigde gegevens. Dit zijn onder meer de vercijferde PIN-code, het bedrag, het rekeningnummer van de klant en een volgnummer. Over het gehele bericht wordt door de security box een cryptografisch controlegetal (een MAC, Message Authentication Code) berekend. Het BeaNet-systeem zal de transactie alleen accepteren indien deze MAC juist is. Daar deze MAC met behulp van een geheime, niet-toegankelijke sleutel wordt berekend, is het niet mogelijk de inhoud van het bericht te wijzigen zonder dat dit wordt gedetecteerd.

Door de aanwezigheid van een volgnummer in de transactie is het niet mogelijk dezelfde transactie meermalen aan BeaNet aan te bieden. Het BeaNet-systeem zal de latere transacties weigeren op grond van het gelijke volgnummer. Wijziging van het volgnummer is niet mogelijk door het bovengenoemde MAC-mechanisme.

Ook het autorisatieresultaat dat door de banken via BeaNet aan de betaalautomaat wordt teruggezonden, is met een MAC beschermd tegen wijzigen. De programmatuur van de security box is zodanig ingericht dat altijd als een positief confirmatiebericht naar BeaNet wordt gestuurd, er ook een positief bericht voor de klant zichtbaar wordt gemaakt.

Fysieke maatregelen

Voor de realisatie van de genoemde bescherming is het noodzakelijk dat de security box is voorzien van een hoge mate van fysieke beveiliging. Het toetsenbord moet een integraal deel uitmaken van de security box en niet kunnen worden afgetapt in verband met de veilige afhandeling van de PIN-code. Ook het display dient, in verband met de controle op de getoonde berichten (zoals "U HEEFT BETAALD"), deel uit te maken van de security box. Daarnaast dienen de aanwezige geheime sleutelgegevens niet toegankelijk te zijn. Dit houdt in dat de security box deze gegevens dient te wissen zodra hij wordt geopend of opengebroken. Ook het wismechanisme zelf mag niet buiten gebruik kunnen worden gesteld. Dit stelt hoge eisen aan het ontwerp.

CONTROLE OP DE MAATREGELEN: CERTIFICATIE

De automaten worden tweeledig op hun juiste werking beoordeeld. Door middel van een conformance-test wordt nagegaan of de automaat goed werkt (hierbij kan worden gedacht aan de juiste berichtenuitwisseling met het centrale systeem en het storingsvrij functioneren). De beveiliging van de automaat wordt separaat en in samenwerking met de banken gecertificeerd.

De controle op de genoemde maatregelen is opgesplitst in een aantal deelgebieden. Elk deelgebied wordt onderzocht door een of meer specialisten en aan de certificatiecommissie gerapporteerd. Deze commissie weegt de verschillende rapporten tegen elkaar af en stelt een eindadvies op. Door deze werkwijze is het mogelijk een goede balans te vinden tussen de verschillende implementaties van getroffen beveiligingsmaatregelen. Hierbij kan het voorkomen dat sterke punten uit een bepaald gebied zwakke punten uit een ander gebied compen-

seren. Als normdocument gelden de Dutch Banks EFT/POS Terminal Specifications, waarin de specifieke eisen voor betaalautomaten zijn aangegeven.

Beoordeling functionaliteit en architectuur

Bij deze beoordeling wordt een onderzoek uitgevoerd naar het functioneel ontwerp van de programmatuur van de security box. Hierbij wordt vastgesteld of de door de fabrikant samengestelde functies de gespecificeerde bescherming bieden. Ook wordt onderzocht of de individuele deelfuncties op een onjuiste manier kunnen worden gebruikt, bijvoorbeeld in de verkeerde volgorde. Verder wordt onderzocht of de (modulaire) opbouw van de security box aan de gestelde eisen voldoet.

Beoordeling implementatie (code review)

Op basis van de resultaten van de beoordeling van de functionaliteit wordt vervolgens de implementatie beoordeeld. Hierbij wordt de programmatuur van de security box in detail onderzocht op de juiste implementatie van de beschreven functionaliteit. Door het aanbrengen van een cryptografisch controlegetal over de programmatuur wordt verzekerd dat de beoordeelde programmatuur gelijk is aan de later in de security box aangeleverde programmatuur. Dit controlegetal wordt door BeaNet bij initialisatie voor elke security box gecontroleerd.

Beoordeling fysieke veiligheid

De fysieke veiligheid wordt door een specifiek laboratorium (zoals TNO) onderzocht. Hierbij wordt onderzocht welke inspanning (zowel financieel als in tijd) benodigd is om de beveiliging van de security box te doorbreken. Het resultaat van dit onderzoek wordt door een aantal specialisten beoordeeld.

Beoordeling procedures authenticiteit en fabricage

In dit onderzoek wordt de methode van produktie en kwaliteitsbeheer bij de fabrikant onderzocht. Indien nodig wordt een bezoek gebracht aan de desbetreffende fabriek. Indien de fabrikant zijn kwaliteitsbeheersing volgens ISO-9000 normen heeft ingericht, betekent dit dat een bepaald basisniveau aan documentatie aanwezig is. De juiste uitvoering van de aanwezige procedures dient echter wel te worden vastgesteld. Tevens worden de procedures die betrekking hebben op de vaststelling van de authenticiteit van de security boxen onderzocht.

CONCLUSIE

Elektronisch betalingsverkeer kent, net als alle andere betaalvormen, een aantal specifieke risico's. De hiervoor genomen beveiligingsmaatregelen zijn zodanig ingericht dat grootschalige invoering met gebruik van een verscheidenheid aan apparatuur mogelijk is. Met de beschreven maatregelen en de daarbij behorende controles is door het Nederlandse bankwezen een effectieve en pragmatische bescherming geboden voor het gebruik van betaalautomaten bij elektronisch betalingsverkeer.

De werkwijze biedt een uitstekende balans tussen flexibiliteit en gerichte functionaliteit, een hoog beveiligingsniveau en aanvaardbare kosten voor leverancier en gebruiker.

LITERATUUR

Normen en richtlijnen

[BeaN91] BeaNet BV, *Dutch Banks EFT/POS Terminal Specifications*, versie 2, 1991.
Dit document beschrijft de eisen die worden gesteld aan een betaalautomaat voor de verwerking van Nederlandse bankpassen. Het bestaat uit een outline en drie appendices, welke de host interface, de user interface en de benodigde beveiliging beschrijven. De specificatie van de beveiliging wordt uitsluitend op need-to-know-basis en onder non-disclosure verstrekt.

[ISO91] ISO, DIS 9564, *Banking - Personal identification number management and security*, 1991.
Dit document beschrijft op welke wijze dient te worden omgegaan met PIN-codes, zowel voor de kaartuitgevende instelling als de controlerende en verwerkende partijen.

E.R. Fekkes
Is werkzaam bij BeaNet op het gebied van informatiebeveiliging. Hij is onder meer voorzitter van de Certificatie Commissie Security boxen BeaNet en is betrokken bij de inrichting van de BeaNet-beveiligingsinfrastructuur.

S.W.I.F.T. and Security

This article was produced by S.W.I.F.T. s.c. Marketing
and the Chief Inspector's Office

Via het netwerk van S.W.I.F.T. worden dagelijks circa 1,5 miljoen berichten uitgewisseld tussen banken, effectenhuizen, vereveningsinstituten en andere financiële instellingen. Inbreuken op de beveiliging van dit netwerk kunnen onvoorstelbare schade tot gevolg hebben. De S.W.I.F.T.-organisatie heeft altijd veel aandacht gehad voor beveiliging.
De auteurs, werkzaam bij S.W.I.F.T., belichten het weldoordachte beveiligingsconcept van deze organisatie en de wenselijkheid van het in gebruik nemen van nieuwe technologie om hieraan invulling te geven.

INTRODUCTION

S.W.I.F.T., The Society for Worldwide Interbank Financial Telecommunication, was established in 1973 and charged with two fundamental responsibilities. The first was to provide a reliable and secure international telecommunications network that would electronically connect the increasingly globalised financial community; and secondly, to develop and maintain standard messages that would be used over the network to support a broad range of financial transactions. These plus operational issues and policy and administrative matters are fully detailed in the S.W.I.F.T. User Handbook which is part of the contractual agreement with users.

Since the start of operation in 1977, the network has grown significantly and today supports the very risky and sensitive business of banks, brokers, exchanges, central depositories and clearing organisations, in over eighty countries. In such business, confidentiality is paramount - consequently, security is a fundamental aspect of the entire S.W.I.F.T. system and is rigorously implemented throughout in order to address the full spectrum of risk.

This article will outline the Society's philosophy about security and how that is translated into practical applications in the day-to-day environment of both the company and its users. In particular, attention will be given to S.W.I.F.T.'s forthcoming release of USE (User Security Enhancement), as well as the focus on security audit that permeates throughout S.W.I.F.T.

S.W.I.F.T. s.c.

Originally conceived as a way of eliminating cumbersome, paper-based systems from the rapidly expanding financial industry, it has proved effective in reducing costs, through automation, and improving security in financial communications.

The Society is headquartered in La Hulpe, Belgium, and has representative offices in New York, London, Rio de Janeiro, Hong Kong and Tokyo, along with two network operating centres: one in Zoeterwoude, Holland and the other in Culpeper, Virginia.

The network currently transmits over 1.5 million messages each day and yearly message traffic growth has averaged fifteen percent over the past five years.

S.W.I.F.T. was initially conceived to automate the financial transaction process through the exchange of structured messages of limited length. This core service is implemented today with the FIN Service (for FINancial messages). An example of FIN will be presented below, but it essentially involves transporting a message from one user to another, checking the format of the message, acknowledging the message's acceptance (if it conforms), storing a copy and, finally, guaranteeing the delivery of the message to its destination.

The Society provides other complementary services:

- Premium, which selects and copies messages to a central point or third party. For instance, messages can be copied to a banking group's head office, central bank or clearing organisation, or national securities depository.
In France, a Large Value Transfer Mechanism, "Transfert Banque de France" is to be operational shortly, which is based on Premium. This will enable banks in France to obtain instant finality of payments executed by the French central bank.

- Ecu Netting, a service initially provided for the Ecu Banking Association, performs a multilateral netting function to provide statement and balance reports to user banks on net payments denominated in Ecu.

- Accord Netting, a confirmation matching and advisory netting service for foreign exchange and money markets.

- And on another independent platform, Interbank File Transfer (IFT) which facilitates the transmission of high volumes of data. So, for instance, a user could transmit electronically, administration and accounting information, customer information, economic data or statistics, general correspondence.

The core FIN service comprises over 130 standardised and computer-readable messages, supporting the principle activities of financial institutions. It covers the following areas:

- Payments & cash management: customer payments, money transfers, statements;
- Trade finance: collections, documentary credits, guarantees;
- Financial markets: foreign exchange, securities markets;
- Syndications;
- Travellers Cheques;
- Administrative messages: charges, interest.

The inherent risk behind any breach of security can result in untold damages and costs.

As an example of the use of these messages, let us look at a simplified chain of events that might be involved in a securities transaction and indicate the S.W.I.F.T. FIN messages used. Note that MT stands for MessageType and each message with a corresponding different purpose, has a different MT number. So for instance, MT500 will contain details relating to an "Order to Buy":

Trading

MT500 An institution (bank, fund manager) instructs its securities broker to buy stock.
MT512 The broker sets up the trade with a counterparty and confirms the trade details with the counterparty.
MT510 Broker confirms to client the details of the trade as well as information specific to the payments side of the transaction.

Settlement

MT520 Broker instructs custodian to receive the purchased securities.
MT530 Custodian confirms all details concerning the receipt of the specified securities.
MT580 Custodian instructs an international clearing system (e.g. Euroclear, Cedel, SICO-VAM, OCC) to carry out the receipt of the specified securities.

Although grossly simplified, the example illustrates the type of information sent and received by the players in this market. Each day around the world institutions engage in the buying and selling of securities, with the value of any single transaction ranging from the very low to the staggeringly high.
The inherent risk behind any breach of security relating to the transmission of information on trades, clearing the trades, ultimate settlement of trades, reporting on trades, etc. can result in untold damages and costs. As such, security at S.W.I.F.T. is taken very seriously and a concept of security is echoed throughout the design of the S.W.I.F.T. network.

NETWORK ARCHITECTURE

S.W.I.F.T. exploits the benefits of many different types of hardware:

- the message switching FIN service is hosted by Unisys A Series mainframes;
- the file transfer IFT service and the value added netting service are implemented on Stratus XA2000 series;
- the worldwide network uses Northern Telecom DPN100 switches administered by a Digital Vax and Sun workstations;
- the subsidiary STS develops bank terminals based on Digital Vax, Unisys B Series, and IBM Series-1 and PS/2 systems.

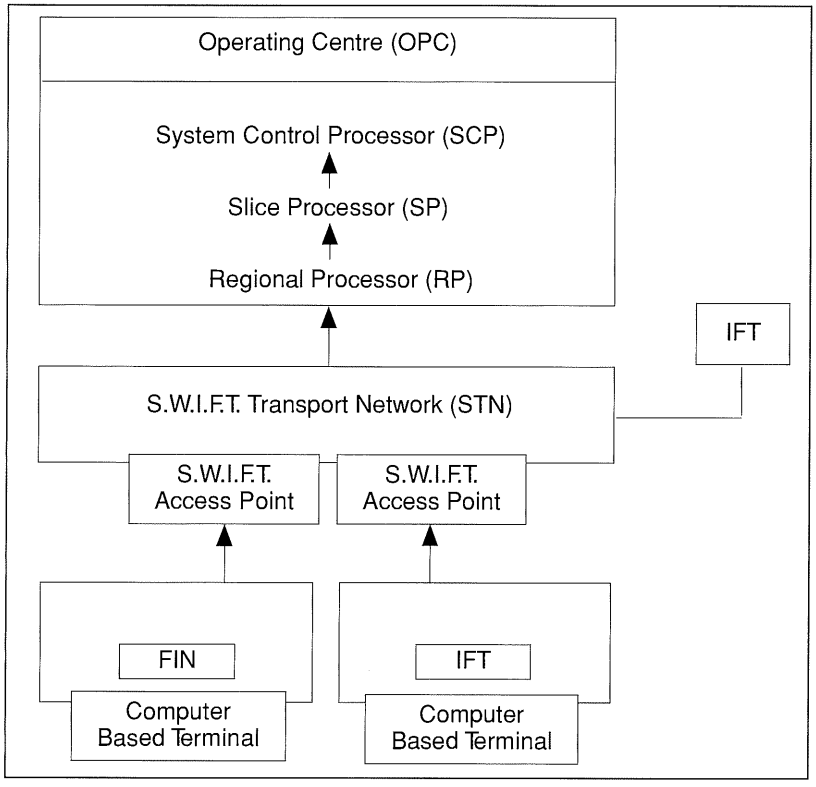


Figure 1. The S.W.I.F.T. Network Architecture.

As illustrated in figure 1 the production system providing the core service, comprises three distinct parts:

1. the user's computer-based terminal, generating messages at the bank via manual entry or via a mainframe link;
2. the transport network, converting the messages into X.25 packets to be transported to one of the two Operating Centres for processing;
3. the FIN and IFT servers at the Operating Centres, to validate, store and forward the messages.

The Computer Based Terminal (CBT) is the terminal which gives the user access to the network. Based on specifications provided by S.W.I.F.T., currently more than one hundred independent companies provide S.W.I.F.T.-compatible hardware, software and consultancy services. In addition, through its S.W.I.F.T. Terminal Services (STS) subsidiary, S.W.I.F.T. itself provides the majority of users with a comprehensive range of terminals and software packages.

The S.W.I.F.T. Transport Network (STN), a vast worldwide web of high-speed, high-capacity data lines, uses the X.25 communications protocol to vehicle the data between the users and the Operating Centres. Users connect their terminals to the transport network via local leased lines and/or dial-up lines which hook into central access points in each country.
These unmanned sites, called *S.W.I.F.T. Access Points* (SAP), forward messages via other SAPs to regional processors. Each SAP is equipped with packet switch equipment to convert S.W.I.F.T.'s proprietary communications protocol to the network's X.25 standard protocol. Equipment is duplicated where necessary to ensure fail-safe system availability, and monitored from the Operating Centres.

The Regional Processors (RP) are located at the Operating Centres and control the flow of traffic by validating the message content for syntax and meaningful parameters and by queueing them for delivery.

Messages are forwarded from the RP to the Slice Processors (SP). Also located at the Operating Centres, the slice processors control the switching of messages and their storage. The SPs perform the actual store-and-forward function, copying every message for guaranteed safe-storage for four months. The safe-storage is acknowledged to the user to confirm reception of the message and that S.W.I.F.T. takes total responsibility for delivery of the message. The message is then directed to the recipient's regional processor to await delivery on request. By virtue of the system's modular configuration concept, additional SPs (slices) can be added, when necessary - giving unlimited capacity to the network.

One System Control Processor (SCP), with a hot-standby in every Operating Centre, monitors and controls all nodes in the network. It also controls all access to the FIN service. SCPs fulfil a variety of tasks including database and software maintenance, logging and report generation.

SECURITY AND RISKS

S.W.I.F.T.'s concept of security follows three fundamental ideas:

- Security is not an objective on its own, but is part and parcel of the mission and activities of the organisation. By defining a Responsibility and Liability policy between the service users (Banks) and the service provider (S.W.I.F.T.) the risks are clearly identified and allocated to either of the three parties; sender, S.W.I.F.T. or the receiver. Risks are allocated based on who is in the best position to control the risk, i.e. the least-cost avoider.

– Security is not isolated at S.W.I.F.T.; the service users must play an active role in whatever security arrangements there are, as defined in the Responsibility and Liability policy. The principle behind the security measures is that of continuity of control, i.e. controls of risks must overlap such that no risks can be caught in the middle.

– Security measures must be practical. For example, they must not hinder the work because this would encourage finding bypasses. Security measures are chosen to provide the highest practical level, i.e. slightly higher than the best level of security found in industry. This results from the fact that one hundred percent security is unattainable and would in any case have an exorbitant price and make the service impractical.

These are the three guidelines that continue to be applied today. Once they are accepted, they need to be reviewed for their applicability in a changing environment; technology advances, knowledge becomes more widespread, changing geo-political risks and erosion of security procedures. It is the Chief Inspector who monitors the strength of the security applied within S.W.I.F.T. and the strength of security measures provided to the users.

Responsibilities for security were discussed by Board committees in the period 1975-1978. These discussions took place within the scope of the development of the Responsibility and Liability policy and the first external security reviews performed by the Stanford Research Institute.

The result was the establishment of the Board Security Review Committee and to statements in the Policy Volume of the User Handbook. It also led to the requirement for an annual external security audit, and the original mission statement of the Chief Inspector:

"The Chief Inspector is responsible for providing overall guardianship for the security and reliability of the company's services, and, for the security and integrity of its internal operations (excluding financial operations)."

In order to ensure the absolute independence of the Chief Inspector in all aspects of his responsibilities, a dual reporting line was established, first to the Board and second to the Chief Executive Officer. As a consequence of the broad ranging requirements imposed by his mission, the Chief Inspector is supported by twelve permanent staff members. They form the Chief Inspector's Office based in La Hulpe headquarters.

Because of his unique position of independence, the Chief Inspector is charged with maintaining the Responsibility and Liability policy under the guidance of the Board R&L Committee. Consequently, he is ideally placed to act as arbiter and interpreter of policy in the event of disputes between users or between users and S.W.I.F.T.

The Chief Inspector's Office is made up of two departments:

– Security Management acts as the guardian of user security - both in its construct and its administration. S.W.I.F.T.'s users will be familiar with this department as it is they who administer the Login tables, respond to claims and advise on technical security issues such as authentication. It is Security Management who implement S.W.I.F.T.'s confidentiality policy. Only they have the authority to grant access to financial messages after specific approval has been obtained from the user.

– Security Audit on the other hand acts as the guardian of S.W.I.F.T. internal security - both in setting security and control policies and in performing audits. The complete segregation of the internal audit function assures absolute independence over all other S.W.I.F.T. functions including that of Security Management. Because thorough independent and expert review is so important in S.W.I.F.T., an additional external security audit is performed each year by a major professional audit firm.

Security is not an objective on its own, but is part and parcel of the mission and activities of the organisation

In addition the Chief Inspector's Office coordinates with external auditors. The external auditors report directly to the Board, and their independent opinion statement on the condition of security in S.W.I.F.T. is carried in the company's Annual Report. The audit firm is commissioned each year by the Board with a mandate to perform a full security audit. This includes a review of the activities of the Chief Inspector's Office.

Similarly the Chief Inspector will, when he considers it appropriate, commission internationally recognised experts to review particular aspects of security, for example in the area of cryptography. This again is in order to bring the users of S.W.I.F.T. further assurance that their security is set at the highest practical level.

The natural consequence of the combination of the three functions - Audit, Advice and Arbitration - within the Chief Inspector's Office results in a synergy of key competencies, and enables the Chief Inspector to comment objectively and authoritatively on all areas relating to security and policy.

In handling claims on the one hand and reviewing S.W.I.F.T.'s security on the other hand, the Chief Inspector's Office is in a position to advise on the need for new or adapted policies on responsibility and liability. Such findings are reported to the Board's R&L Committee which will propose policy changes to the full Board. Such policy statements are contractually binding responsibilities documented in the User Handbook.

The Chief Inspector's Office also proposes recommendations for users to discharge their responsibi-

lity adequately via the S.W.I.F.T. Newsletter and broadcasts messages (i.e. messages to all users). To make security between users practical and efficient while secure, the Chief Inspector's Office also gives guidelines through the same media and in individual responses on queries.

The principles taken into account in defining the Responsibility and Liability policy, which is one of the major added values of the S.W.I.F.T. service, are:

- the notion of a preventable risk is not reasonable when the users do not know the risk, do not know about frequency and impact, or do not have choice as to cost/benefit aspects;
- continuity of control, by having overlapping controls between parties such that problems can be caught;
- prevention of risks, by assigning the responsibility to the party in the best position to evaluate the impact and the frequency of the risks;
- least cost avoider, by assigning responsibility to the party in the best position to avoid the risk.

S.W.I.F.T. is responsible:

- if a message is acknowledged to the sender and is undelivered, but does not appear in undelivered message report;
- if there is a system or personnel failure;
- if users are not notified promptly of failures in Operating Centres and Regional Centres.

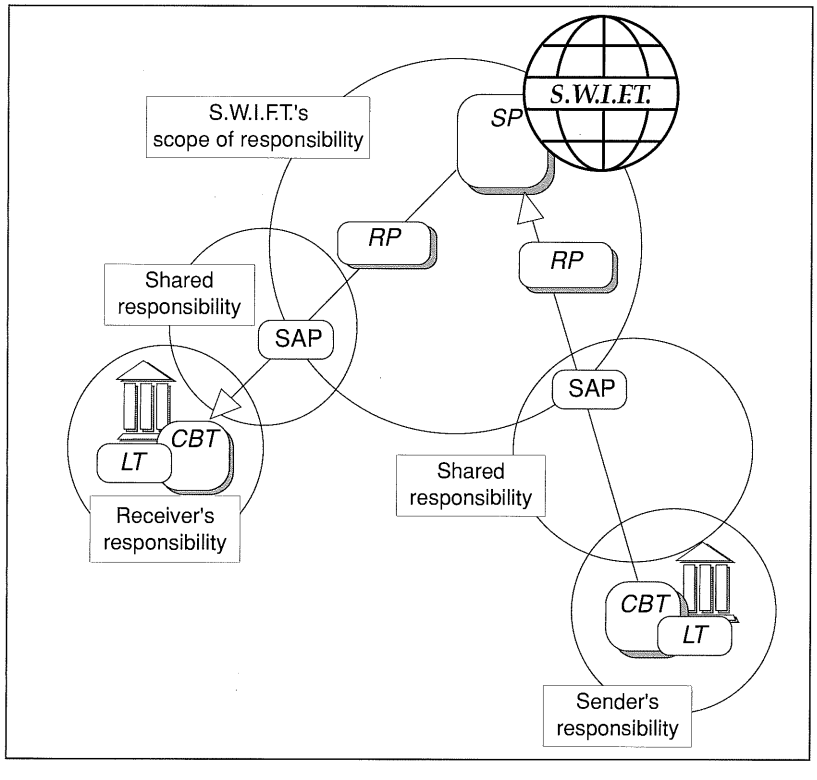
Sender is responsible:

- if S.W.I.F.T. does not acknowledge the message;
- if a message is acknowledged but appears on the undelivered message report;
- if the sender does not react appropriately to S.W.I.F.T. message status notifications;
- if S.W.I.F.T. does not return a delivery notification prior to reciever's cut-off time for an urgent message;
- if the transaction does not have the proper format when a prescribed standard exists;
- if the sender does not react promptly to S.W.I.F.T. notifications of failures.

Receiver is responsible:

- if a message addressed to its BIC destination and received prior to cut-off time is not processed with correct value;
- if the receiver does not adhere to the Terminal Policy. This policy requires that users have backup terminals to at least receive urgent traffic;
- if the receiver has not completed an adequate Output Sequence Number (OSN) reconciliation to ensure receipt of all messages;
- if the receiver does not react promptly to S.W.I.F.T. notifications of failures;
- if the receiver does not query "problem" messages as soon as feasible.

Figure 2. Responsibilities.



SECURITY OBJECTIVES

For the purposes of correctly describing and categorising requirements in the security of a system, each of the three key security elements, Confidentiality, Integrity and Availability form separate sections:

1. *Confidentiality*, which means that information is only disclosed to authorised persons at authorised times in authorised locations. It implies prevention of unauthorised disclosure of information.

2. *Integrity*, which means that information can be relied upon to be complete, accurate and valid. It implies prevention of unauthorised modification of information.

3. *Availability*, which means that information and the associated service is accessible and usable when needed. It implies prevention of unauthorised withholding of information.

It must be noted that these security objectives only deal with *information*. It is not the intention to protect systems per se, but rather the information they process through information technology.

Because the systems in question are not to be sold but are to be operated to provide a service, there is a fourth security objective. An additional objective, because the system is not only developed and installed, but also put into operation. This objective therefore does not deal with information itself but with the persons accessing the system:

4. *Accountability*, which means that every individual authorised to use the system must be made

accountable. This implies he is uniquely and provably identified and monitored for his activities on the system.

The user accountability requirement is to cover situations where access to information was indeed authorised (the first three objectives) but was misused, i.e. a dishonest act of an employee. Dishonest acts or fraud have created the most losses in the industry.

For the core service, the three components of information security are further broken down into two levels:

1. *User data*, i.e. the information contained in a single message and the information contained in a sequence of messages, which are to be processed by the core service. This means security on a message-by-message basis respectively on a destination-by-destination basis.

2. *System Data*, i.e. the information defining the systems, which implement the core service. This includes hardware parameters, telecommunication lines topology, programs, databases, configuration data, usercodes, and encryption keys. For every new system it is decided up front what is sensitive data (level of confidentiality) and critical data (the need for it for proper operation).

The security objectives are closely related to *service quality* objectives. For example, if information needs to be accurate it should not be corrupted, if it needs to be valid it must be presented in a meaningful way, if it needs to be accessible the system should not fail due to a bug. It is thus not only the quality of the system itself that is addressed but also the quality of its supporting administration and operation systems.

The *Security Objectives*, i.e. the confidentiality, integrity and availability of information, are endangered by *Security Threats*, i.e. the risks from outside or inside, which are to be managed by *Security Controls*, i.e. the technical and managerial mechanisms.

The risks vary from environmental casualties, acts of terrorism to collusion within S.W.I.F.T. staff, and include force majeure, failures, fraud, errors and omissions. The security controls to counter these, can be subdivided into four layers under control of the Company.
An example of contractual controls is the use of non-disclosure agreements, of organisational controls is the segregation of duties, and of procedural controls the sign-off of certain requests.

Technical controls are those mechanisms to enforce certain controls or to prevent unauthorised access. These are the controls to be implemented by a system but, in practice, they need to be complemented by controls on the other layers. For example, encryption is only effective with proper procedures for the management of the encryption key. Timebombs cannot be one hundred percent prevented and technical protection needs to be complemented by contractual fidelity clauses. Authorisation of commands is only effective when there is a proper segregation of duties.

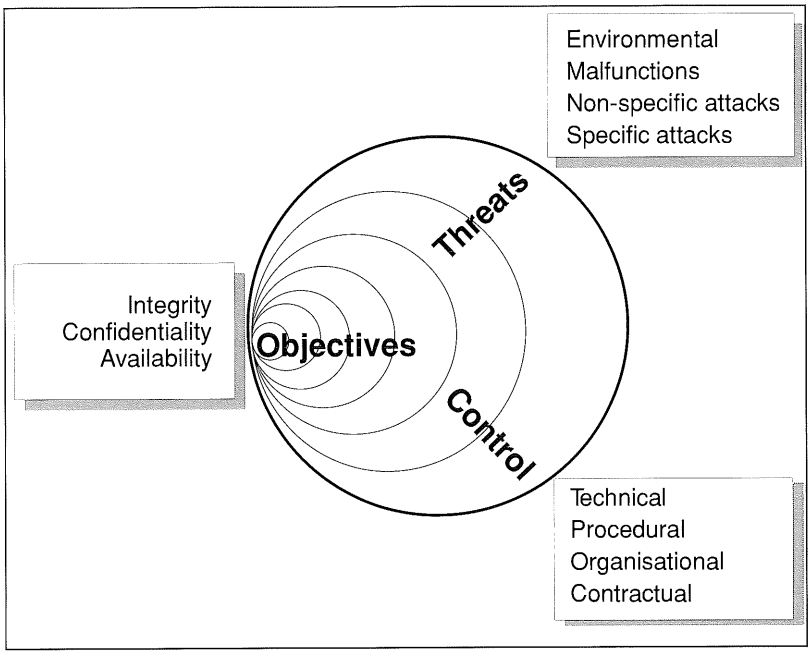


Figure 3. Security Objectives, Threats and Controls.

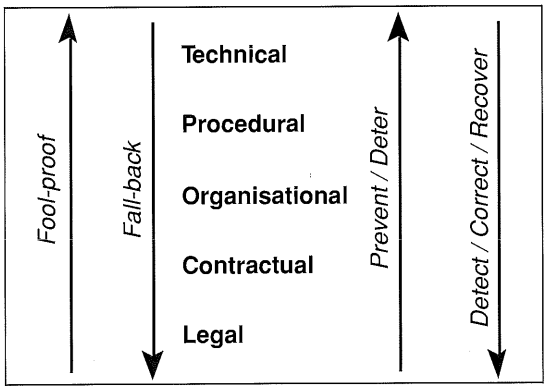


Figure 4. Security Controls.

The following sections begin with an analysis of the security objectives, followed by general security controls described in more detail.

SECURITY CONTROLS

Every user message processed by S.W.I.F.T., is and remains owned by the sender and is specifically destined for one addressee. This leads to the following: for every acknowledged message, S.W.I.F.T. s.c. takes full responsibility including financial liability for accuracy, completeness and timely delivery. In other words, S.W.I.F.T. provides assurance

and guarantee that there is (unless properly notified):

- No wrong delivery
  (delivery to another user would be a major confidentiality breach);
- No double delivery
  (payments would be executed twice);
- No late delivery
  (would incur associated interest loss);
- No corrupted delivery
  (leaving message contents intact);
- No false delivery
  (fraudulent messages);
- No lost delivery
  (messages not delivered and hence not executed);
- No disclosed delivery
  (messages are private and extremely confidential);
- No rearranged delivery
  (messages are delivered in correct order).

To control the extremely high business risks associated with this responsibility, S.W.I.F.T. introduces specific security controls. On the one hand, security controls within the system (S.W.I.F.T.-System Controls) and on the other hand security controls to be implemented by the user and in the service provided by S.W.I.F.T. between the user and S.W.I.F.T. (user-S.W.I.F.T. Controls).

S.W.I.F.T.-SYSTEM CONTROLS

Confidentiality

User-data

A user message is restricted information under S.W.I.F.T. definitions and thus may not be read nor copied in clear, except by the sender and receiver. The only exception is where for the purposes of investigation or arbitration the sender or receiver may authorise S.W.I.F.T. to view specified messages. In this regard, the Chief Inspector's Office is designated mediator between the users and S.W.I.F.T. for ensuring that formal authorisation is obtained.

Internal procedures dictate that an illegal entry into a site must be checked, logged and if considered suspect, the site must then be isolated.

Although not defined as "restricted", traffic analysis falls under the company confidential definition. Traffic analysis is the determination of the volume of messages exchanged between banks or the number of certain messages types used by a bank, or alternatively the volume of traffic exchanged between countries.

All international telecom links between S.W.I.F.T. Transport Network nodes are encrypted by means of bitstream encryptors. These bitstream encryptors use session keys which are changed very often and generated based on a master key. Every link has its own master key.

Internal procedures dictate that an illegal entry into a site must be checked, logged and if considered suspect, the site must then be isolated. SAP isolation means that no new messages are accepted from users and all messages in transit are rerouted via other SAPs. For regular support of lines, the local support staff use customised datascopes. These datascopes filter out all characters contained in the message contents and leave all protocol data intact for display.

Messages are software-encrypted after validation at the input-RP and remain encrypted while in safe storage, i.e. the SP does not see messages in clear. Messages are only decrypted at the output-RP prior to delivery. A Trace command exists which is capable of tracing and reading the messages of a particular line terminal. This command however blanks out all message text just the same as with the customised datascopes.
In the event the message text itself is needed for support, explicit approval from the sender is sought and confirmed by the Chief Inspector's Office. This is done through a digital signature scheme, whereby the command to display message text is only activated by the system after it receives the correct signature. Only Security Management have the authority and technical ability to achieve this and because of this unique capability, which is realised through digital signature techniques, the Chief Inspector's Office is on-call to provide this authorisation on a 24hour / 7day a week basis.

System-data

On the systems level, confidentiality means the protection of sensitive operational data, a pre-requisite for all other security objectives. This is partially achieved by a combination of physical and logical access controls. Satisfactory implementation of access controls requires the proper protection of all the secrets for authentication and encryption.

The Login and Select keys are never shown in clear to staff. These keys are generated from a seed which is entered into the S.W.I.F.T. database via Admin messages generated by an offline, secret database. The controls associated with Admin are exactly the same as with user CBTs. In fact, the link between the database and network is regarded as a bank connection and is done through a CBT.

Source code is also considered company confidential. The major reason is that any weakness in the software could be exploited by a hacker. In order to reduce this risk, knowledge of the source code and access to the object code should be kept to a minimum. To achieve this, developers work in a strictly physical access controlled area from which no tapes or microcomputers may be removed, without explicit approval.

Integrity

User-data
A user message is owned by the sender and classified as restricted information, its contents may not be changed or corrupted. This means that in no situation should a message be altered, not even for correcting a "mistake". If an alteration is detected, it should be notified to the sender and the message discarded.

Not only the message itself must remain integral but also the entire context of messages sent or received by a user. This means that messages should not be lost, should not be delivered to a user other than the addressee, nor fraudulent messages inserted. This relates to service accountability and results from the responsibility taken by S.W.I.F.T. for direct loss.

An end-to-end checksum is recalculated at every intermediate node to protect messages against accidental or telecom corruption.

Changes to messages are not possible because the live system does not contain tools which can edit messages. Editors and compilers are just forbidden on the production network and even made impossible thanks to a proper security set-up.

In S.W.I.F.T., strict sequence control over messages is achieved by automated sequence number checking, both on input and output. In fact, it is S.W.I.F.T. that manages sequence numbers per user. Once a message is detected to be out of sequence, not only is the message rejected; the whole session is aborted forcing the user to re-authenticate himself. This effectively protects against insertion, deletion or replacement of messages.

It is S.W.I.F.T.'s policy to be accountable for the total traffic at all times, including such events as system and database failures. This means that after serious system problems messages should not be lost or duplicated unless notified to the users. S.W.I.F.T. has implemented some very sophisticated recovery schemes with different levels to make sure no message is lost. From a physical point of view, all vital disks are mirrored and copied onto tape-cartridges every five minutes.

System-data
System integrity control protects the system from unauthorised system changes. This means that the set-up of the system in terms of programs, configurational data and access control data, can be at all times relied upon. This requires, for example, proper protection against viruses and timebombs and proper reviews of patches, to maintain program integrity. Configurational data includes for example the usercodes, the closed-user-groups, the definition of access ports, the authorisation schemes, and the set of destinations.

Configuration data is managed on an offline database. This database is the source feeding the system database and the STN network database. The three databases administering the network configuration are kept permanently synchronised. An authorisation scheme provided by the Admin application ensures that updates are first approved by the owner of data, such that the master database can be updated accordingly.

In S.W.I.F.T., a strict procedure is applied for the release of the numerous programs and configuration files which constitute a new release. The changes are created on a network isolated from the live network. After qualification, any program or configuration file changes are stored in a special patch database, which is managed by a specialised Configuration Management entity. This Configuration Management group releases new code files via tape to the live system where a SysDir mechanism checks the presence of software and verifies a checksum. The checksum is calculated after all patches are released to Configuration Management. The SysDir checks the presence and version of code files. Furthermore, the development environment is isolated from the live network and physically protected. Some sensitive utilities, changing the network configuration and usercodes are specifically protected.

Availability

User-data
Availability of a message means that the message should be delivered in a timely manner. This results from the responsibility taken for indirect loss. Timely means that value-date messages must be delivered prior to the cut-off time of the receiver. As a rule messages should be in the output queue within a minute. This means that message availability really becomes a function of performance, and failure to deliver messages exposes the Company to user claims for indirect loss.

Balancing input and output can conflict with the system availability objective.

Availability of traffic means that a user can login both when and for how long he wishes and can send and receive all his messages. As such, traffic availability is the service availability perceived by a particular user.

Control over message availability, i.e. its timely delivery, can be accomplished through proper flow control between input and output. It must be noted that balancing input and output can conflict with the system availability objective, which in S.W.I.F.T. is defined as the amount of time input can be accepted, and not by the amount of time output can be delivered.

System-data
The application availability index reported by

S.W.I.F.T., is in fact the system availability. It is per definition the amount of time the systems are able to accept input of new messages.

A resilient system may result paradoxically in increased time-to-detect.

In order to specifically spot bottle-necks and weaknesses and to define specific requirements, the availability index is split into five constituent parts:

1. Time Between Failures,
which is defined as the time that the network runs without a "fatal" failure.

This requirement is subdivided per node and per link and differentiates between major and minor failures. Note that the time-between-failures is not equivalent to the time-between-outage, because redundancy built in the network might mask a single failure.

In assessing the availability of a system, there is a strong relationship between (1) the time-between-failure, (2) the duration of an outage and (3) the impact or scope of an outage, e.g. the number of users directly affected. The latter two factors are considered as the "severity" of a failure.

2. Time To Detect,
which means the time between the occurrence of the bug and the realisation of the severity of the problem.

To provide a high quality service, the time-to-detect should be lower than the time-to-complain, i.e. a failure should have been noticed and reported internally before a user complains. To reduce the time-to-detect, the system provides specific alarms or events. Moreover, the operator workstation filters these alarms, such that only important alarms are sent to the operators. This reduces the communication of unnecessary information to the Operators and alerts them immediately to critical events.

3. Time To Investigate,
which means the time needed after escalation to isolate and find the problem.

To reduce the time-to-investigate, two factors are important. On the one hand, staff involved are trained to have the proper knowledge, there is proper on-site presence and proper escalation procedures oriented at quick problem determination and solving. On the other hand, specific investigation tools and investigative data, and appropriate and up-to-date documentation are available. Also, release notices and listings with database changes are maintained and easily accessible in an automated format.

4. Time To Recover,
which means the time taken to solve the direct problems and bring the network up, i.e. time spent on remedial action, such as activation of new software and recovering those nodes directly affected.

The time-to-recover is almost entirely dependent on the system capabilities, redundancy and performance, although proper instructions for the operators are a vital element. Therefore, the recovery paths are specifically documented in an automated fashion and clearly indicated how and when they should be used.

5. Time To Normalise,
which means the time taken to solve the consequential damage, and to bring the network back into its original state.

The time-to-normalise is generally not taken into account in availability calculations. Nevertheless, a problem which is not solved in depth, might cause downtime at a later stage, thus indirectly affecting availability.

In the first stage of a failure, a problem occurs or a complaint is registered. This is the *incident*, which is then investigated to find the *defect* causing it. At this stage an immediate fix is generally provided, to re-establish operations. S.W.I.F.T. recognises that a defect that has caused the incident needs to be solved in depth and that somebody must still be held responsible for making sure the defect is corrected. This stage is where the definitive solution is implemented and is called *normalisation.*

For example, a software bug can be corrected by a new release of software, or a temporary patch-cord can be removed following a corrective database update, or a faulty link can have been repaired by the PTT. Therefore, an organisation is set up such that someone formally assumes the *ownership* of problems, such that not only the immediate fix of a problem is done, but also its proper normalisation.

Note that all these times are not specified per "node" but rather on a service level, i.e. the set of nodes and links comprising the whole system. Recovery times, however, can be specified on a node basis as they are primarily a performance issue.
The SCP has two hot-standby Monitor-SCPs, one in the same Centre and an other one in the other Centre. It must be noted that the Monitor-SCPs are only effective for hardware failures or to speed up recovery.
The SPs are backed-up by a hot-standby in Brussels. Safestorage disks on the SP and the system disks are duplicated. These disks are copied about every five minutes on to two sets of tapes. One set is kept on site, while another is kept off-site.
The RPs are put in a pool with a ratio of one warm-standby RP per two active RPs. STN nodes are not really duplicated in their entirety, but all vital elements are duplicated inside.

The network systems generally contain more than one version. Obviously, only one version is active, but in case a failure can be attributed to a change recently brought in, a previous version of the software can be activated. The SysDir lists the object files currently active on a particular host.

USER-S.W.I.F.T. CONTROLS

Referring back to figure 2, we see that global system security is a shared responsibility and both the user and S.W.I.F.T. must play their role to protect against unauthorised access. S.W.I.F.T.'s responsibility is for the operation and security of the network, to assure the availability of the service and to maintain the integrity and confidentiality of sensitive information and of messages after reception at the S.W.I.F.T. Access Point (SAP).

The provision of CBTs, their connection to the SAP, and activities within the user organisation are the responsibility of the user. For the benefit of all users, it is necessary for S.W.I.F.T. to make recommendations and regulations concerning these matters.

Figure 5 illustrates the four major security controls provided on the network in order to control the grey area of responsibility between S.W.I.F.T. and its users. These are:

1. User-to-Swift encryption (e.g. STEN) as a confidentiality control in the area between the user and the closest S.W.I.F.T. Access Point. It is a protection against someone attempting to read or disclose messages from or to a user. This is provided by a hardware encryption device attached at both ends of a user's leased line.

2. User-to-Swift sessions (Login, Select) as a logical access control and as a first level of authentication of the sender. It is a protection against someone attempting to send or receive messages in lieu of a legitimate user.

3. User-to-Swift sequencing (ISN and OSN) as an integrity control of the traffic exchanged between S.W.I.F.T. and a user. It is a protection against someone attempting to duplicate, to insert or to intercept messages from or to a user.

4. User-to-User authentication (MAC) as an integrity control of messages and a second level of authentication of the sender. It is a protection against alterations of messages or the introduction of false messages. It guarantees to a receiver that the message was not altered during its transit through the S.W.I.F.T.-system and the local lines.

The controls overlap a bit in order to not rely completely on one specific control.

The following sections will present S.W.I.F.T.'s implementation of security for the user connecting to S.W.I.F.T. The focus of S.W.I.F.T.'s forthcoming User Security Enhancement (USE) project is on two

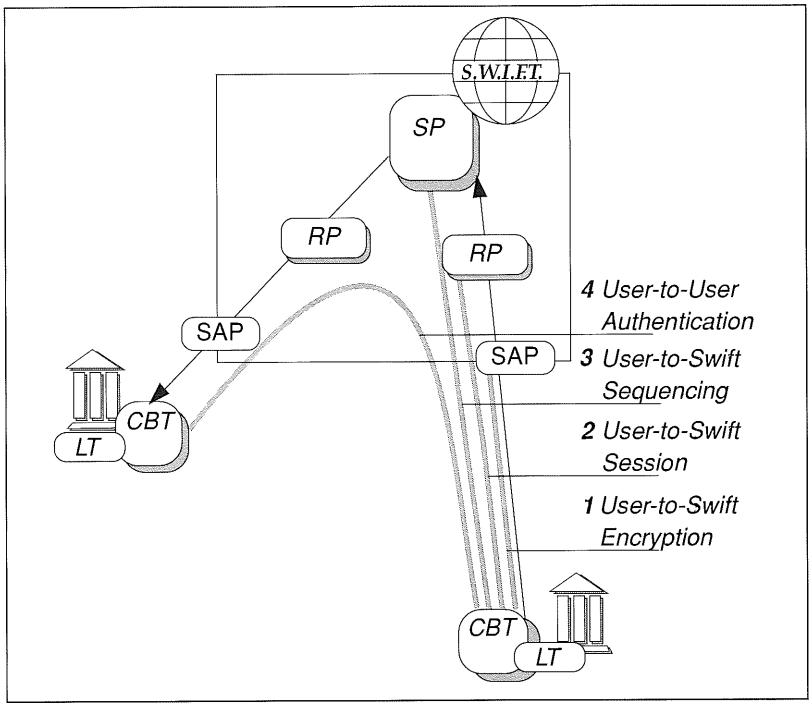


Figure 5. Four major security controls.

vital aspects of security within the user's domain. These are: firstly, session authentication (control of logical access to the network); and secondly, the exchange of message authentication keys between correspondent financial institutions. Although these security controls have always been available over S.W.I.F.T., their implementation has been largely a manual routine:

- control of access to the network is achieved by paper-based Login codes which are issued by S.W.I.F.T. and read or typed into the terminal;
- the exchange of authentication keys between counterparties is typically done by way of mail or telex correspondence.

USE - A NEW SECURITY ARCHITECTURE

Under the User Security Enhancement project (USE) two new services will be introduced to respond to the security needs identified above for both logical access and key exchange. Both services provide enhancements to existing security procedures, namely:

- paper-based Login tables to gain access to S.W.I.F.T. services will be replaced by Integrated Circuit Cards, more popularly known as "Smart Cards";
- paper-based exchange of bilateral authentication keys will be replaced by exchanging secured messages over the S.W.I.F.T. network.

Essentially, the implementation of USE requires two pieces of hardware: A Secure Card Reader and an Integrated Circuit Card (ICC). Pictured in figure

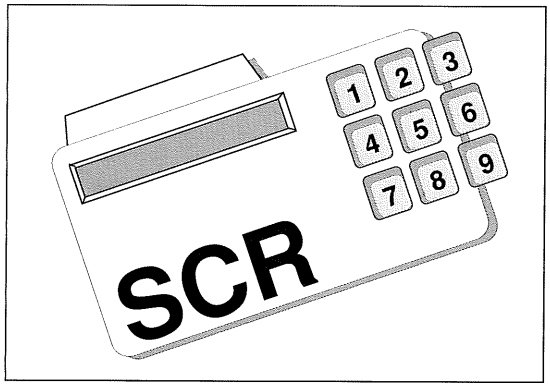


Figure 6a. Graphic of SCR.

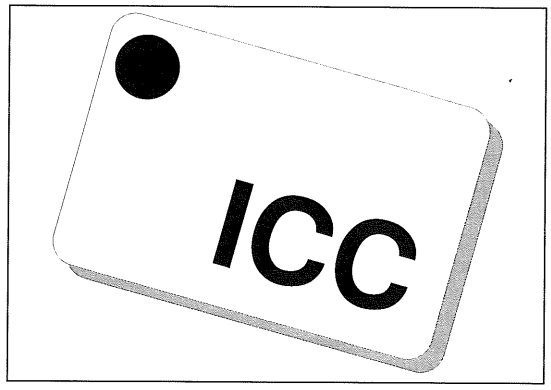


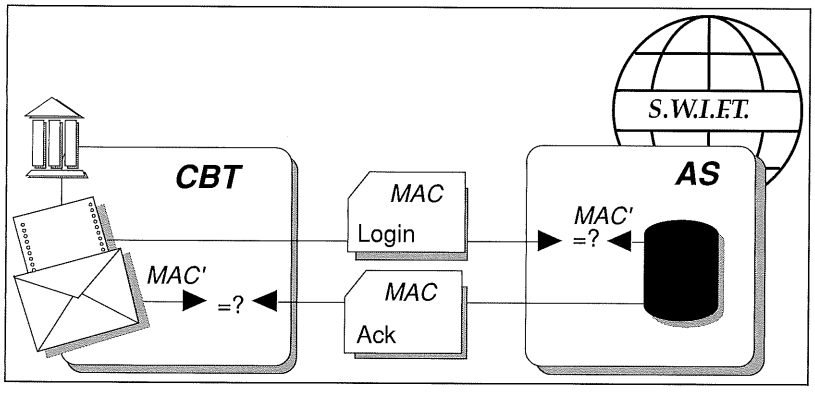
Figure 6b. Graphic of ICC.

6, the reader is a "tamper resistant" device consisting of an outer casing, keypad and display and a slot into which an ICC may be inserted. It is the ICC which contains the user-specific secrets. The reader is supplied by S.W.I.F.T. and contains the software for the cryptographic functions and for reading from (and writing to) the ICCs.
The reader holds, or has access to, all keys and algorithms and performs computations using those keys and algorithms. In addition, there is a back-up card reader which is solely used for the Login/Select function.
The Integrated Circuit Card, which resembles a typical bank/credit card, contains all of the functional elements of a microcomputer - a microprocessor, both burned-in and programmable memory and external interface allowing input and output of data:

- 8 bit microprocessor with 128 byte RAM,
- 4 kbyte ROM and 8 kbyte EPROM,
- S.W.I.F.T. proprietary mask for encryption algorithm.

It is made tamper-resistant and cannot be read nor copied, i.e. the microprocessor controls the memory access. The ICC can only operate when inserted into a card reader and requires the use of a PIN (Personal Identification Number) or two PINs, as a measure of further protection.

Figure 7. Session authentication with Login.



Session authentication (login protocol)

Initially, the user accesses the S.W.I.F.T. network via the Login function. The purpose of Login is to identify and authenticate the Logical Terminal (LT) to S.W.I.F.T. and to confirm to the LT that it is in fact communicating with S.W.I.F.T. and not some other network, e.g., one that is fraudulently emuating S.W.I.F.T.

This is achieved by the exchange of a one-time code. This code is calculated based on the actual Login and on the keys printed on the paper-based Login tables mentioned previously. This code can therefore be generated (and verified) only by S.W.I.F.T. and the user concerned.

From a security perspective this protocol is good practice and achieves a high degree of security. Its obvious weakness however is that the Login tables, distributed in hardcopy form, require handling and are visible to the human eye. The next section explains how USE addresses this weakness.

Session authentication (USE Secure Login/Select)

With USE, the paper-based Login access codes will be derived from a suitably configured ICC and these codes will be read by the reader, which is in turn connected to the S.W.I.F.T. terminal. The terminal can then use these access codes in the normal way to gain successful access to the appropriate S.W.I.F.T. application (e.g. FIN).

With USE, improvements in the administration of access control functions are derived because an ICC is configured for individual use by one responsible person within the user's organisation. Further, once configured, an ICC is capable of generating thousands of access requests without any user intervention. Operationally, since with USE users need not read or type access codes, nor have to decide which codes are the correct codes to use; the possibility for error is eliminated.

Paper-based Login tables can be copied, lost, damaged and easily used by an unauthorised individual if not securely controlled. However, the use of USE ICCs improves the security of logical access

due to the fact that ICCs are "tamper-resistant", cannot be copied or read, and are more robust than paper. Further, the use of the ICC is protected by a PIN.

Message authentication

In order for a financial institution to act upon a received instruction to, for example, buy/sell a certain security, or perform the process of settling a securities trade, the receiver of the instruction(s) must be confident of its origin, as well as the content and the authority of the message. Therefore, counterparties, or correspondents, will agree to exchange numeric keys as a way to "sign" or authenticate the messages they send to each other. Currently this exchange of keys is done independently of S.W.I.F.T. and a particular key is generally only used for a finite period after which new keys must be exchanged.

The key is used as a "seed" for the algorithm which when applied against the contents of the FIN message results in a unique value. This value is then appended to the message being sent. Recalculating this arithmetic value at the receiver's end and comparing it to the value appended to the message (from the sender's end) allows the receiver to confirm that the mes-sage has not been tampered with or changed.

Why message authentication?
Providing a tool for verifying:
- the identity of the sender;
- the integrity of the message content.

What is message authentication?
By calculating an authentication based on:
- the message content;
- a standard and mandatory algorithm;
- the secret key shared by the sender and the receiver (unknown to S.W.I.F.T.) - this effectively means a *user-to-user* security control.

How is message authentication done? By one-way hashing type of encryption (see figure 10).

The message authentication is a custom designed algorithm with the fol-lowing key properties:
- *Symmetrical*
  i.e. with keys which are the same on both sides (shared bilateral keys);
- *One Way*
  i.e. it is impossible to decrypt - or alternatively to figure out the key with the known text and result;
- *Unpublished*
  i.e. it is a S.W.I.F.T. proprietary design published only to terminal developers.

Message authentication has the following cryptographical characteristics:
- statistical properties, to make the result unpredictable after changes in the text or key;
- text sensitivity, to make every minor or major change to the text visible;
- key sensitivity, to discourage guess-ing or progressively finding the key;

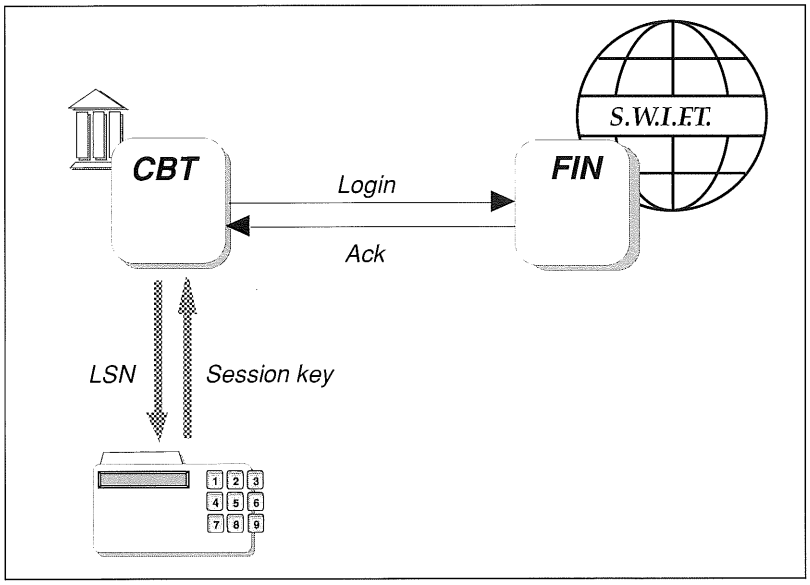


Figure 8. Session authentication with USE.

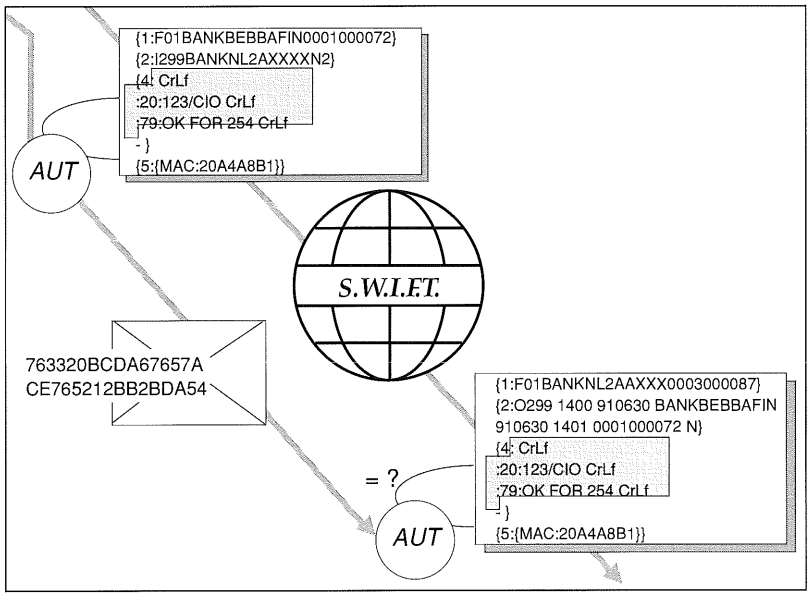


Figure 9. Message authentication.

- key length is such as to discourage exhaustive key search;
- irreducible and irreversible algorithm, in order to prevent reverse engineering or hard-ware optimisations.

Again, from a security perspective, the use of keys achieves an excellent degree of verification that messages have not been tampered with. The problem is, however, that the administrative and operational load associated with generating and securely distributing such keys (remember, each correspondent will require a different key) may result in reduced security at the level of operations. This is where USE provides a solution.

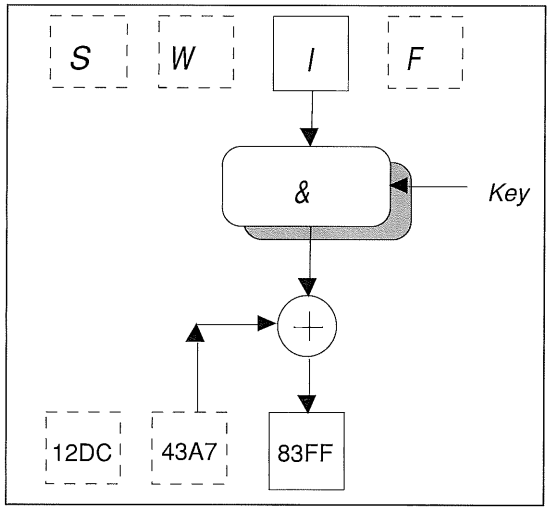


Figure 10. One-way hashing type of encryption.

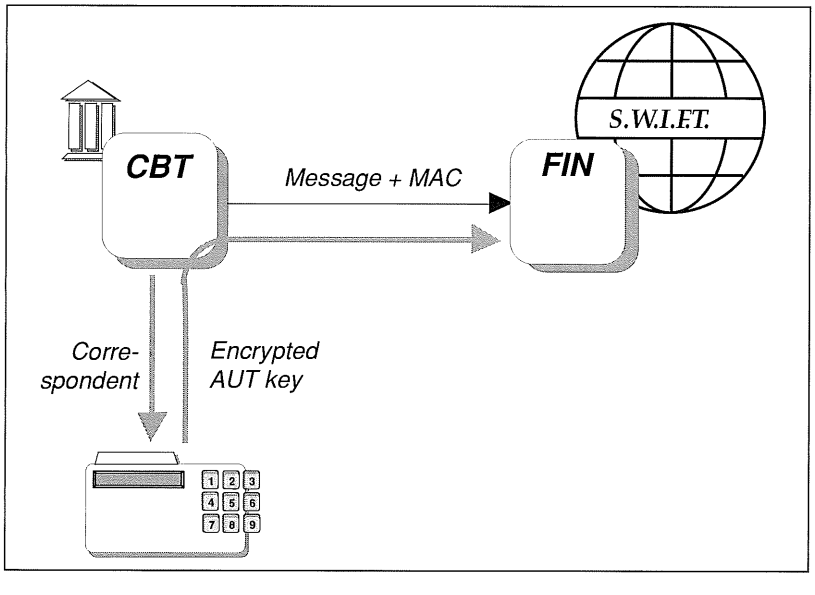
Message authentication (USE Bilateral Key Exchange)

The major impact of USE is that key exchange will be automated. This will not only reduce the cost of implementing security, but also improve security directly as well as indirectly by easing the operational and administrative burden.

USE will replace the manual and tedious system of generating and exchanging bilateral authentication keys between users. With USE the keys will be generated inside the Card Reader and encrypted before being passed on to the S.W.I.F.T. terminal to which the SCR is connected, see figure 11.

The terminal then automatically exchanges the key with the correspondent by way of four new S.W.I.F.T. FIN messages. Essentially the four messages are:

Figure 11. Generation of authentication key.



1. a request for the correspondent's public key;
2. correspondents public key;
3. generation and transmission of proposed bilateral authentication key to correspondent;
4. acknowledgement of receipt and verification of key.

Once the key has been exchanged and verified it is stored within the S.W.I.F.T. terminal of both correspondents for use in authenticating S.W.I.F.T. messages.
This enhancement of the current method of bilateral key exchange provides users with significant administrative and security-related advantages. Certainly the greatest administrative advantage will be in removing the requirement for paper-based correspondence, and at the same time enabling greater control over the key exchange process itself. The direct security benefits include:

- keys will not be visible to an operator;
- keys will be transported safely;
- keys cannot be copied;
- the identity of a correspondent can be checked.

Furthermore, the bilateral key will be secret to both bilateral partners, and S.W.I.F.T., and the operational simplicity of the system means that correspondent partners will be prepared to exchange keys more regularly, thereby reducing the risk of compromise.

The USE project will be a major milestone in user security. The removal of manual and paper-based procedures will facilitate a streamlining of operations. In addition, a tighter and more easily administered security routine should result in reduced costs in implementing required security.

THE CHIEF INSPECTOR'S OFFICE

The Chief Inspector's Office prime role is to provide independent opinions on security to the Board and the Executive. They assess the degree of security and control applied in the organisation in respect of its mission, i.e. the timely, secure and accurate transmission of financial information.

To form an independent opinion, audits are performed covering the whole company. There are three levels of audit, Project Audit which reviews a project's lifecycle, Product Audit which reviews the product itself, and Operational Audit which reviews the product in its live environment. Briefly considering each level:

Project Audit
A pro-active approach is applied in auditing projects. This consists of proposing security and control policies to the Executive for company-wide application, and, of advice to project teams in the early project phases. This advice concentrates on security practices and techniques to be applied in the development process, the development environment and operation of the function. Project audit concentrates on quality assurance, the correct re-

porting of progress and adherence of the project to proper development lifecycle standards.

Product Audit
Product Audit assesses whether the security functions and mechanisms satisfy the security requirements. The audit reviews the suitability of functionality, synergy between functions, consequences of known and discovered vulnerabilities and ease of use. This effectiveness evaluation builds upon the correctness assessment of the project audit.

Operational Audit
Obviously, the pro-active approach needs to be supplemented with traditional post-implementation compliance audits and with a continuous security monitoring of the live systems. Operational audit assesses whether proper responsibilities are assigned for the management of sensitive data, applications and equipment, whether proper segregation of duties is applied and whether sufficient alarms and audit trails exist and are reviewed. In addition, every data centre is subject to internal audit at least once every year and every regional centre at least once every three years.

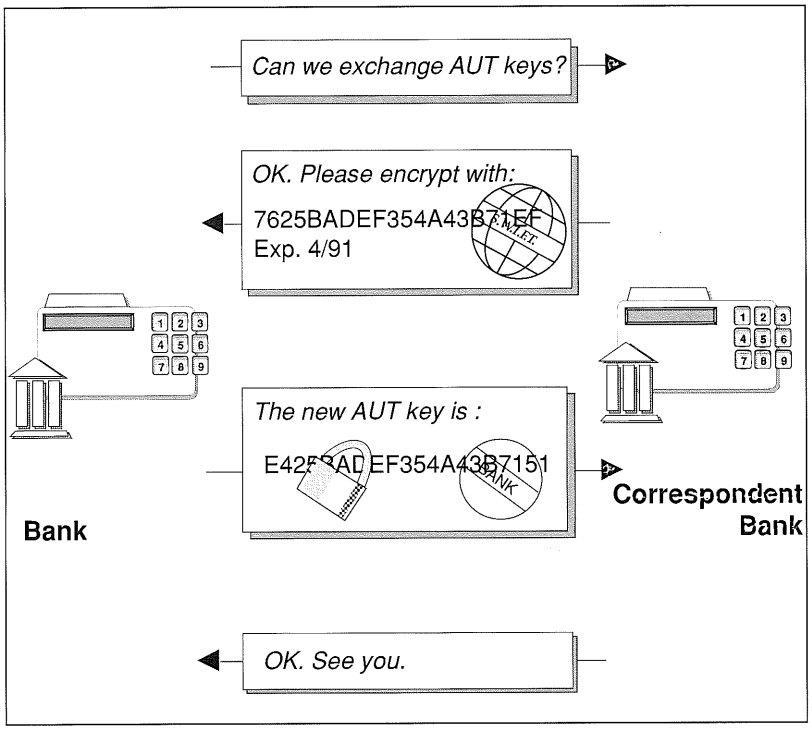


Figure 12. Exchange of authentication key.

Independence

The direct reporting line of the Chief Inspector's Office to the Board and the CEO avoids potential bias or concealment of major findings. Results are summarised for the Board with an indication of the management response. For major projects like Swift-II, internal audit reports are also issued to the relevant Board Committees. All audit reports are kept available in the Chief Inspector's Office Available to all Board Members.

To assure independence, the complete functioning of the Chief Inspector's Office is reviewed by External Auditors on a yearly basis.

It should be noted that the Chief Inspector's Office has an advisory role, responsibility is and remains with the project teams and ultimately with the management of the company. Also the monitoring role of the Chief Inspector's Office does not waive this responsibility from operations, support and administration.

Because of this, and to strengthen security in a distributed environment, Security Administrators and Security Coordinators have been appointed within the Company's divisions where appropriate. The segregation of operational security responsibilities from those of the Chief Inspector's Office enable internal audit to perform regular and independent compliance reviews. The Security Administrator function consists of setting up and maintaining a secure environment. This is done by limiting access privileges, refining the operations as a balance between security and operability, providing instructions and educating users on how to organise themselves securely, and, coordinating both with other security administrators and with the Chief Inspector's Office.

Advice

A specialised function has been set up within the Chief Inspector's Office which monitors all user security related projects, advises in their development and participates in their verification stages. These projects are usually complex and employ advanced technology and techniques such as changes to hardware encryptionand as seen above for USE.

Where necessary, the Chief Inspector's Office also engages external expert consultants, typically in the area of cryptography. They independently assess whether the techniques used offer users the best level of security. Their results are also summarised in the Chief Inspector's Report. Examples of this are the regular vetting of S.W.I.F.T.'s authentication algorithm, the encryption algorithms applied throughout S.W.I.F.T. and the lifetime of security keys.

Because it has gathered the experience over the years, the Chief Inspector's Office will advise on principles, design and even propose detailed technical approaches. Advice at early stages is considered much more cost-effective than to recommend changes as a result of subsequent audits. The responsibility for design and implementation is and remains however with the project teams and ultimately with the management of the company.

CONCLUSION

As the volume and complexity of international financial transactions continue to rise, the need for information security in terms of confidentiality, integrity, and availability also increases - it is not difficult to appreciate the added risks associated with global financial dealings, particularly in today's environment of scarce resources. This situation is further compounded by a need to control the cost of operational and administrative practises throughout the finance industry.

S.W.I.F.T. was founded as a cooperative Society to allow banks to share the high cost of a state of the art network system. The Society continues today to provide reliable, cost effective, timely and secure solutions to its member's (user's) needs relative to the standardization, simplification and processing of data between each other.
S.W.I.F.T.'s User Security Enhancement is designed to further extend the role of the Society to meet these needs. That is, providing significantly greater control over operational and administrative procedures and thereby reducing the risk of fraud or error; providing increased security, and reducing the cost of implementing network security.

As indicated in this article, the importance of security and control of risk permeates the provision of telecommunications services by S.W.I.F.T. In particular, the role of the Chief Inspector in overseeing a company and network-wide audit to ensure security and control. The responsibility S.W.I.F.T. assumes with respect to using the network goes so far as to provide arbitration in disputes between a sender and receiver, or to a claim by a user against S.W.I.F.T. - in the case of the latter, S.W.I.F.T. will assume financial responsibility and i unique in this respect.

S.W.I.F.T.'s User Security Enhancement is designed to further extend the role of the Society to meet these needs. That is: providing significantly greater control over operational and administrative procedures and thereby reducing the risk of fraud or error; providing increased security, and reducing the cost of implementing network security.

Het binnenlandse traject van SWIFT-posten; het SWIFT-8007-circuit

Drs. F.G. Knaack

Het gemiddelde transactiebedrag van posten in het SWIFT-8007-circuit bedraagt circa ƒ 4 miljoen, en in 1991 ging het om een totaalbedrag van bijna ƒ 8 biljoen. Het 8007-circuit betreft de afwikkeling van betalingen in Nederlandse guldens waarbij niet-ingezetenen zijn betrokken.
De beveiligingsmogelijkheden van dit betalingsverkeer zijn mede afhankelijk van het medium en voor een deel facultatief. Knaack, die bij de BankGiroCentrale onderzoek verrichtte naar dit circuit, geeft aan dat het optionele karakter van de beschikbare beveiligingsvoorzieningen een afbreukrisico inhoudt.

INLEIDING

Internationale betalingen kunnen worden afgewikkeld via het zogenaamde SWIFT-netwerk. S.W.I.F.T. is de afkorting van Society for Worldwide Interbank Financial Telecommunication. Internationale betalingen die het gevolg zijn van handelingen met geldautomaten, betaalautomaten en eurocheques kennen ieder hun eigen "circuit".
De transacties in Nederlandse guldens waarbij de opdrachtontvangende bank in Nederland een bedrag moet overmaken naar, of ontvangen van, een andere deviezenbank, worden verrekend via de BankGiroCentrale (BGC) en worden onder de code "8007" door de deviezenbanken gerapporteerd aan De Nederlandsche Bank. Dit binnenlandse traject van SWIFT-posten wordt het SWIFT-8007-circuit genoemd. Het wordt alleen gebruikt wanneer een Nederlandse bank een andere Nederlandse bank als tussenpersoon heeft voor het ontvangen of versturen van een SWIFT-post. Momenteel wordt dit circuit beheerd door de BGC. De posten dragen deze naam omdat binnen dit circuit de indeling van de posten gelijk is aan de door S.W.I.F.T. gehanteerde standaardindelingen.

Transactievolume

De betekenis van dit soort transacties blijkt uit de relatief zeer hoge bedragen die ermee gemoeid zijn. In 1990 was dat ƒ 5.253 miljard, in 1991 ƒ 7.862 miljard; het gemiddelde transactiebedrag bedroeg daarbij circa ƒ 3,9 miljoen. Deze transactievolumina nemen al enige jaren flink toe.
Teneinde de toegang tot dit SWIFT-8007-circuit voor kleinere banken te vergemakkelijken is in de loop van 1990 de mogelijkheid geopend om via een BGC-PC de SWIFT-posten aan te leveren.
Eind 1990 maakten 61 banken in Nederland gebruik van dit circuit.

Ontwikkelingen

De centrale banken wensen zelf de verantwoordelijkheid te dragen voor betalingsverkeer waarbij de transactiebedragen zeer hoog zijn. Mede in dit kader heeft De Nederlandsche Bank, na overleg met de betrokken banken, besloten om de verwerking van de SWIFT-transacties in Nederlandse guldens op zich te nemen. Vooralsnog zal dit gebeuren met gebruikmaking van de bestaande infrastructuur. Voor de deelnemers zullen er zo min mogelijk veranderingen plaatsvinden.

In dit artikel zal worden ingegaan op de functie van het SWIFT-8007-circuit, de processen die de SWIFT-posten ondergaan en de beveiligingsaspecten van dit betalingscircuit.

BESCHRIJVING VAN HET SWIFT-8007-CIRCUIT

In deze parafgraaf wordt een aantal aspecten van het SWIFT-8007-circuit beschreven.

Doel van het SWIFT-8007-circuit

Het SWIFT-8007-circuit heeft de volgende doelen:
- het doorleiden van SWIFT-8007-posten, afkomstig van een Nederlandse bank, naar een andere Nederlandse bank;
- het verzorgen van de verevening van de betrokken bedragen;
- het verzorgen van zodanige opgaven aan DNB dat de controle uit hoofde van de voorgeschreven deviezenverantwoording kan worden vereenvoudigd.

Het SWIFT-8007-circuit dient het verzorgen van zodanige opgaven aan DNB dat de controle uit hoofde van de voorgeschreven deviezenverantwoording kan worden vereenvoudigd.

Daarnaast geldt nog eens dat de posten in principe onherroepbaar zijn: een bank kan besluiten de voor het vereveningstijdstip ontvangen posten uit te voeren. Een bank die toch een post wenst te herroepen, dient hiervoor bepaalde procedure-afspraken in acht te nemen.
Wanneer de SWIFT-8007-posten binnen één Nederlandse bank gerouteerd worden, kan deze bank zelf de opgave aan DNB verzorgen.

Soorten SWIFT-8007-posten

Momenteel worden als SWIFT-8007-posten bij de BGC verwerkt:

a. alle posten in Nederlandse guldens waarbij een niet-ingezetene betrokken is (deviezenmeldingsplichtige opdrachten);

b. verrekeningen in Nederlandse guldens uit hoofde van wisselarbitrage tussen ingezetenen waarbij de inzendende bank één van de betrokken partijen is. Dit wordt gedaan uit efficiëntie-overwegingen (niet-deviezenmeldingsplichtige opdrachten);

c. rentevergoedingen behorende bij SWIFT-8007-transacties (niet-deviezenmeldingsplichtige opdrachten).

ad a. Voorbeelden van deviezenmeldingsplichtige SWIFT-8007-posten zijn:

1. bankbetalingen, onder andere:
   - saldoreguleringen door een buitenlandse bank;
   - verrekeningen uit hoofde van arbitrage- en depositotransacties met buitenlandse banken;
   - dekkingsopdrachten uit hoofde van het blanco buitenlandse betalingsverkeer.

2. cliëntbetalingen, onder andere:
   - blanco buitenlands betalingsverkeer ten gunste of ten laste van relaties van binnenlandse banken;
   - verrekeningen met niet-ingezetenen uit hoofde van arbitrage of cheques.

Voorbeelden van niet-deviezenmeldingsplichtige SWIFT-8007-posten:

ad b. verrekeningen tussen deviezenbanken uit hoofde van een wisselarbitragetransactie tussen deze deviezenbanken;

ad c. terugvaluteringen ofwel rentevergoedingen met betrekking tot SWIFT-8007-transacties.

Enkele voorbeelden van het traject van bank- en cliëntbetalingen worden grafisch weergegeven in de figuren 1 tot en met 4.

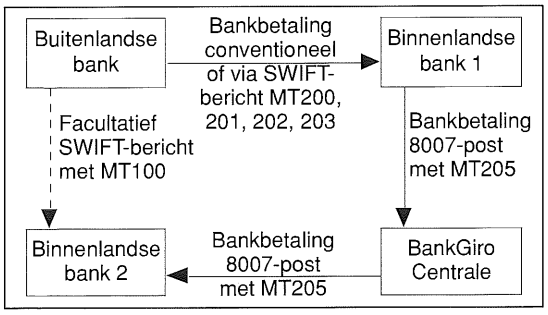
Onder bankbetalingen worden betalingen verstaan die door de banken zelf worden geïnitieerd.

Er wordt in het SWIFT-8007-circuit een drietal berichttypen (Message Types - MT) gehanteerd. Deze zijn afgeleid van de in het internationaal betalingsverkeer gebruikte berichttypen, te weten:

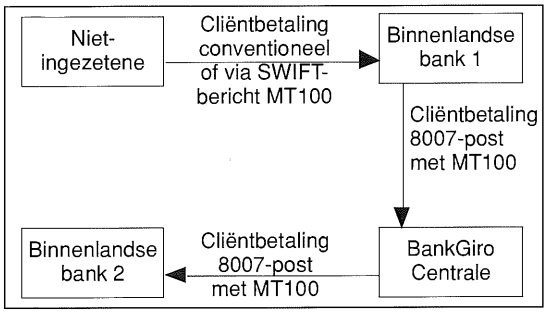
- MT100 - cliëntbetaling welke door de inzendende bank is aangemaakt naar aanleiding van:
  1. een van de cliënt ontvangen betalingsopdracht;
  2. een van een andere bank ontvangen cliëntbetaling;
  3. een banktransactie waaruit een betaling ten gunste van een niet-bank voortkomt.

- MT202 - bankbetaling ten gunste van een derde bank welke door de inzendende bank is aangemaakt naar aanleiding van:
  1. een banktransactie waaruit een betaling ten gunste van een bank volgt;
  2. een andere betalingsopdracht die langs deze weg wordt afgedekt.

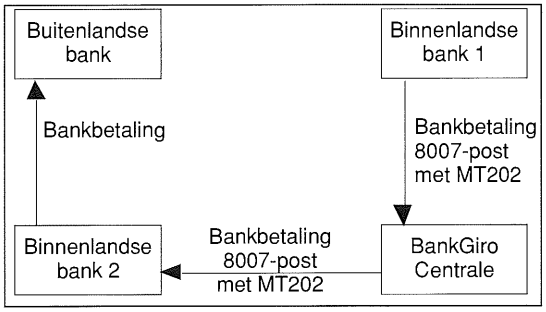
- MT205 - bankbetaling gegenereerd uit een cliënt- of bankbetaling.
Het betreft hier een clearing-bankbetaling die volgt uit een door de inzendende bankinstelling ontvangen bankbetaling ten gunste van een derde bank (MT202 of MT203) of een regulatie (MT200 of MT201).



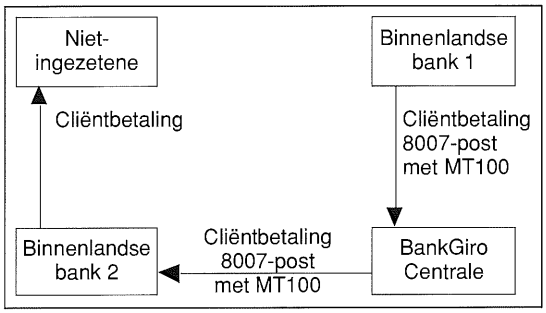
Figuur 1. Bankbetaling vanuit buitenland.



Figuur 2. Cliëntbetaling vanuit buitenland.



Figuur 3. Bankbetaling naar buitenland.



Figuur 4. Cliëntbetaling naar buitenland.

Functie BGC als beheerder

Functies van de BGC voor het SWIFT-8007-circuit zijn:
- de BGC is het centrale punt waar de betrokken partijen de SWIFT-8007-posten via verschillende media kunnen aanleveren respectievelijk van ontvangen;
- de BGC verzorgt centraal de vereveningsberekeningen voor DNB;
- de BGC verzorgt een deviezenmelding bij DNB, uit hoofde waarvan de deviezenmelding van de banken aan DNB kan worden vereenvoudigd.

Beschikbaarheid

Er wordt per werkdag in het BGC-computercentrum te Amsterdam één SWIFT-run (verevening) gedraaid, omstreeks het middaguur, waarin de SWIFT-8007-posten worden verwerkt die 's ochtends voor de verevening, of op de middag en avond van de (werk)dag voor de dag van verevening zijn aangeleverd.

Indien door technische storingen of andere oorzaken het computercentrum in Amsterdam niet bereikbaar is, neemt het BGC-computercentrum in Leusden de taak over en kan in Leusden worden aangeleverd.

In het uitzonderlijke geval de BGC door machinestoring niet in staat is de vereveningstotalen op tijd te vervaardigen zullen aan de hand van de door banken aangeleverde geleidegegevens, waarop totalen per bank staan vermeld, door de BGC de vereveningstotalen worden bepaald en aan de vereveningsfunctionarissen van de banken en aan DNB worden doorgegeven.

Indien één of meer banken posten aanleveren op een zodanig laat tijdstip dat de posten niet meer in de verevening van de desbetreffende dag kunnen worden verwerkt, worden de te laat aangeleverde posten dezelfde dag op initiatief van de bank betaald via het FA-RC-systeem (een DNB-infrastructuur) en wordt de desbetreffende postinformatie met de berichten van de volgende dag aan de banken doorgemeld.

AANLEVEREN BIJ DE BGC

Banken die willen deelnemen aan het SWIFT-8007-circuit van de BGC dienen zich eerst aan te melden, waarna een check-in-procedure volgt.
Een bank kan voor het aanleveren gebruik maken van één of meer media. Zij heeft hierbij de keuze uit tape, datacommunicatie (host to host) en de BGC-PC.

De BGC werkt momenteel nog met twee BankgiroDatacomSystemen (BDS):
- BDS-oud (BSC-protocol);
- BDS-nieuw (SNA-protocol).

Als backup of uitwijkmedium voor aanlevering van posten kan ieder genoemd aanlevermedium dienen. Diskette is het medium dat als backup voor aanleveren via de BGC-PC kan worden gebruikt.

Per bank kunnen meerdere regiocentra, computercentra, etc. input aanleveren. Bij het verstrekken van output door de BGC wordt per bank standaard één toezendingsadres gebruikt.
Het aanleveren van input geschiedt afhankelijk van het gebruikte medium in Amsterdam of in Leusden.

Tape en cartridge

Indien een bank SWIFT-8007-posten aanlevert op tape of cartridge is het noodzakelijk voor de bank om één of meer procuratiehouders aan de BGC op te geven die gemachtigd zijn de begeleidende stukken bij de tape te ondertekenen.

Een deelnemer in de verevening moet zorg dragen voor voldoende dispositieruimte zodat een eventuele debetpositie voordat de verrekening bij DNB plaatsvindt, is afgedekt.

Iedere aangeleverde tape of cartridge bevat minstens één batch met SWIFT-8007-posten. Bij elke batch op de tape of cartridge is een geleidebrief in duplo gevoegd, getekend door een daartoe bevoegde functionaris (procuratiehouder). Indien een bank dit wenst wordt de handtekening op de geleidebrief geverifieerd met het bij de BGC aanwezige bestand handtekeningen. Iedere aangeleverde tape en cartridge wordt ingelezen en gecontroleerd.

Datacommunicatie

SWIFT-8007-posten kunnen batch-gewijs met het BDS naar de BGC worden verzonden.
Batches die via datacommunicatie worden aangeleverd, kunnen vergezeld zijn van geleidegegevens die in een aparte batch (onafhankelijk van de batch met SWIFT-8007-posten) worden aangeleverd. Een andere methode voor beveiliging is het toevoegen van een hash-code (integriteit van gegevens) en het toevoegen van een elektronische handtekening (authenticiteit aanleveraar).
Het BDS heeft uitsluitend een transportfunctie. Na ontvangst van de batch bij de BGC wordt via het BDS elektronisch een ontvangstbevestiging naar de bank gestuurd. Vervolgens vindt er een formele controle plaats of de batch aan de voorgeschreven specificaties voldoet.

BGC-PC

Een aparte vorm van datacommunicatie vormt de BGC-PC. Dit medium zorgt ervoor dat zonder eigen automatiseringsinspanning, decentraal en snel, eventueel vanaf meerdere locaties, afhankelijk van het aantal BGC-PC's dat een bank heeft, SWIFT-8007-posten kunnen worden ingezonden.
De BGC-PC is tevens geschikt als backup-voorziening voor (BDS) mainframe-verbindingen.

Diskette

Aanleveren van SWIFT-8007-posten op een 3,5 inch diskette is alleen toegestaan indien transport via de BGC-PC niet mogelijk is. Indien voor deze oplossing wordt gekozen, kunnen de posten te laat zijn om nog te worden meegenomen in de verevening.

DE VEREVENING

De verevening (clearing) van het SWIFT-8007-verkeer wordt iedere werkdag te zamen met het overige BGC-betalingsverkeer in één verevening om uiterlijk 14.00 uur door de BGC aan DNB aangeboden.
Dit betekent dat een deelnemer in de verevening moet zorg dragen voor voldoende dispositieruimte zodat een eventuele debetpositie voordat de verrekening bij DNB plaatsvindt, is afgedekt. De totale clearingstand, bestaande uit de SWIFT-8007-stand en de vereveningsstand, wordt dagelijks door de BGC aan de deelnemende banken om circa 12.30 uur doorgebeld.

Om de Nederlandse correspondentbank van de begunstigde in staat te stellen zo spoedig mogelijk de informatie over de SWIFT-8007-posten door te zenden is het voor banken mogelijk om vervroegde boekingsoutput, voor de verevening, op te vragen.
Is het voor de BGC door een machinestoring of anderszins niet mogelijk vereveningstotalen op te bouwen, dan zal een noodprocedure in werking treden, teneinde toch nog (handmatig samengestelde) vereveningstotalen door te geven aan de deelnemende banken alsmede aan DNB.

Niet voldoen aan vereveningsverplichtingen

Het is mogelijk dat DNB de BGC inlicht dat de verrekening niet gelukt is met als reden dat het saldo van een bank ontoereikend is, terwijl de boekingsoutput van de BGC reeds in het bezit is van een bank.
In dat geval treden de bepalingen van het vereveningsreglement in werking.

Deviezenmelding

Met betrekking tot de deviezenmelding van de BGC kan onderscheid worden gemaakt in de melding aan DNB en de melding aan deelnemende banken.

Deviezenmelding van BGC aan DNB
Dagelijks worden totalen gecumuleerd door de BGC; deze worden maandelijks opgegeven aan DNB. De opgegeven tellingen betreffen het totaal

aantal posten debet en credit met bijbehorende totaalbedragen.
Voor de melding aan DNB worden alleen de deviezenmeldingsplichtige posten met bijbehorende bedragen geteld.

Deviezenmelding van BGC aan deelnemende banken
Iedere werkdag ontvangen alle banken van de BGC een lijst met deviezentotalen. Deze lijst bevat de deviezenmeldingsplichtige totalen van die werkdag (gespecificeerd naar valutadatum), alsmede het deviezenmeldingsplichtige totaal (cumulatief) voor de lopende maand.
De eerste dag van de nieuwe maand is de lijst van de voorafgaande maand volledig en bevat zij de totalen zoals de BGC deze maandelijks aan DNB meldt. Een bank is met behulp van deze lijst in staat haar eigen gegevens over de opgebouwde totalen te verifiëren aan de totalen zoals deze door de BGC zijn berekend.

OUTPUT ONTVANGEN VAN DE BGC

De boekingsoutput is op verschillende momenten van de dag in verschillende vormen voor de banken beschikbaar.
Per deelnemende bank kan op één plaats boekingsoutput worden ontvangen. Vooraf wordt door de bank aangegeven via welk medium en op welke locatie bij een normale gang van zaken ontvangen wordt.
Als backup voor ontvangst is elk ander genoemd medium mogelijk. Daarnaast is papier als backupmedium voor ontvangst mogelijk.
Ontvangen via datacommunicatie kan zowel vanaf het computercentrum Amsterdam als vanaf Leusden geschieden. Dit is afhankelijk van de gekozen datacommunicatieverbinding.
Ontvangen via de BGC-PC gebeurt via het computercentrum te Leusden.
Tapes en papier zijn afkomstig van het computercentrum te Amsterdam.

Tape

Per aflevertijdstip wordt één batch aangemaakt op tape met daarin alle SWIFT-8007-posten.
In deze batch bevinden zich alle (goede en geweigerde) door de desbetreffende bank aangeleverde posten (debetposten) en alle (alleen) goede posten die voor de bank bestemd zijn. De debetposten worden ook wel teruggemelde posten genoemd, zijnde een terugmelding van de BGC van de aanlevering van een bank. De creditposten worden ook wel doorgemelde posten genoemd. Deze creditposten zijn aangeleverd door een andere bank en door de BGC doorgemeld aan de desbetreffende bank.
De tape gaat vergezeld van een geleidelijst met vermelding van het aantal posten debet en credit en de som van de bijbehorende bedragen.

Datacommunicatie

Per bank wordt per aflevertijdstip één batch aangemaakt. De batch via datacommunicatie bevat, naar keuze van de bank, al dan niet de goede debetposten (terugmeldingen). De batch bevat in ieder geval alle geweigerde debetposten en alle creditposten (doormeldingen) bestemd voor die bank.

De BGC biedt de service dat voor banken gedurende vijf werkdagen de mogelijkheid bestaat duplicaat-output op het gebruikelijke ontvangstmedium aangeleverd te krijgen.

BGC-PC

Voor het ontvangen van output met behulp van de BGC-PC geldt hetzelfde als bij de andere datacommunicatie-aansluitingen.

Papier

Papier wordt door de BGC gebruikt als backupmedium voor het verzenden van boekingsoutput. In het geval dat output op papier wordt aangemaakt, betreft dit alleen creditposten (doormeldingen bestemd voor de desbetreffende bank) en geen debetposten (terugmeldingen van door de desbetreffende bank aangeleverde posten) of geweigerde debetposten.

Duplicaat-output

De BGC biedt de service dat voor banken gedurende vijf werkdagen de mogelijkheid bestaat duplicaat-output op het gebruikelijke ontvangstmedium aangeleverd te krijgen. De banken zullen zichzelf (indien en voor zover nodig) met de archivering van aangeleverde en ontvangen posten moeten belasten, aangezien door de BGC, extern, geen navraagmogelijkheid voor SWIFT-8007-posten wordt geboden.

Melding overzicht output van BGC aan banken

Iedere werkdag ontvangen alle deelnemende banken van de BGC een overzicht met de totalen van de SWIFT-8007-posten die de BGC die dag heeft verwerkt. Dit overzicht bevat het totaalbedrag en het totaal aantal posten per valutadatum.

BEVEILIGING

Het SWIFT-8007-circuit kent meerdere media waarmee transacties kunnen worden getransporteerd. Daardoor kent het circuit beveiligingsmogelijkheden die veelal afhankelijk zijn van het soort medium waarvan gebruik wordt gemaakt. Dit is in tegenstelling tot de beveiligingsprotocollen die door de S.W.I.F.T.-organisatie worden gebruikt en één medium, het datacommunicatienetwerk, betreffen.

Integriteit/authenticiteit

Batches met SWIFT-8007-posten kunnen op twee manieren worden beveiligd. Ten eerste door te werken met totaalgegevens die via een andere weg aan de BGC worden verzonden, ten tweede door gebruik te maken van elektronische versleuteling en hashing.

Controletotalen
De eerste methode is om diverse controletotalen van de batch opnieuw in een onafhankelijke aparte geleide-batch, op papier of via een aparte datacomsessie, te versturen. Deze totalen moeten gelijk zijn aan de batch-totalen.

Voor het binnenlandse circuit is het afhankelijk van het gebruikte medium van welke beveiligingsattributen gebruik wordt gemaakt en waar de verschillende verantwoordelijkheden beginnen.

Het sturen van geleidegegevens in een aparte batch is een beveiligingsmethode die voor ieder medium kan worden gebruikt, met uitzondering van de BGC-PC. Wordt aangeleverd met behulp van de BGC-PC, dan dwingt het systeem tot het gebruik maken van de tweede methode, die hieronder wordt beschreven.

Elektronische sleutel
De tweede methode bestaat uit het beveiligen van gegevens met een elektronische sleutel.
Deze beveiliging omvat twee onderdelen. Het eerste onderdeel bestaat uit het versleuteld meezenden van totaalgegevens, een hash-code, om de integriteit van de gegevens te waarborgen. Het tweede onderdeel bestaat uit een elektronische handtekening, die wordt gegenereerd op basis van de hash-code en het totaalbedrag van de SWIFT-batch. De generatie ervan vindt plaats met behulp van een chipkaart en een chipkaartlezer, waarvan het gebruik door middel van een PIN-code is geïndividualiseerd. Het tweede onderdeel waarborgt de authenticiteit van de gebruiker.

Voor het aanleveren via BDS-oud kan naast een geleide-batch uitsluitend een hash-code als beveiliging worden gebruikt.
Voor het aanleveren via datacom met BDS-nieuw is het mogelijk - afhankelijk van de gebruikte hardware - behalve de hash-code ook de elektronische handtekening te gebruiken. Deze integriteits- en authenticiteitskenmerken vervangen het gebruik van de aparte geleide-batch.

Encryptie

Voor het aanleveren via datacom met BDS-oud en BDS-nieuw bestaat tevens de mogelijkheid om de gegevens versluierd, door middel van encryptie, over de lijn te zenden. Deze versluiering is mogelijk via een modem en kan plaatsvinden na afspraak met de BGC.

Controle van aangeleverde batches

Als een batch ontvangen is door de BGC vindt er een aantal controles plaats. De volgende mogelijkheden doen zich voor:
- technische controles wijzen uit dat de batch niet leesbaar is (voor tapes en diskettes);
- de batch is leesbaar en moet aan specifieke inhoudelijke eisen voldoen.

Indien aan alle voorwaarden is voldaan, wordt de batch geaccepteerd. Indien aan één of meer voorwaarden niet is voldaan, worden passende maatregelen genomen. Het is dan mogelijk een printout van de fout per fax te ontvangen.

VERSCHIL TUSSEN HET NATIONALE EN HET INTERNATIONALE SWIFT-CIRCUIT

Tussen het binnenlandse en het internationale SWIFT-circuit bestaan verschillen. Welke dat zijn, komt in deze paragraaf tot uitdrukking.

Het internationale SWIFT-circuit

De S.W.I.F.T.-organisatie stelt een netwerk ter beschikking. Hierdoor is het medium waarvan het datatransport gebruik maakt beperkt tot datacommunicatie.
S.W.I.F.T. is verantwoordelijk voor de betrouwbaarheid en continuïteit van het gehele netwerk. De aangesloten banken zijn verantwoordelijk voor het aansluitende gedeelte vanaf hun eigen computers tot aan het SWIFT-netwerk, in technische zin tot aan de Communicatie Processor van SWIFT. Voor dit gedeelte zijn de banken dan ook verantwoordelijk voor bijvoorbeeld encryptie en het verzorgen van backup.

Het binnenlandse SWIFT-8007-circuit via de BGC

Voor het binnenlandse circuit is het afhankelijk van het gebruikte medium van welke beveiligingsattributen gebruik wordt gemaakt en waar de verschillende verantwoordelijkheden beginnen.
In het algemeen kan worden gesteld dat de BGC uitsluitend bij het gebruik van de BGC-PC verantwoordelijk is voor het totale traject vanaf de verzendende bank tot aan de ontvangende bank.
Voor de overige media draagt de BGC uitsluitend de verantwoordelijkheid over haar eigen verwerking, "vanaf de brievenbus". Hoe het traject Bank - BGC wordt beveiligd, is afhankelijk van de wens van de individuele banken die al dan niet van bepaalde opties gebruik kunnen maken.

BGC-PC
Indien gebruik wordt gemaakt van de BGC-PC stelt de BGC een fysiek beveiligde PC ter beschikking, waarop applicaties aanwezig zijn die de integriteit en authenticiteit van de betalingstransacties waarborgen, en de sessies op het traject Bank - BGC cryptografisch beveiligen. De bank is verantwoordelijk voor het gebruik en de locatie van de BGC-PC, terwijl de BGC verantwoordelijk is voor de betrouwbaarheid en continuïteit van het traject Bank - BGC, de verwerking, en vice versa.
De getroffen beveiligingsmaatregelen zijn ook van toepassing wanneer in een noodsituatie gebruik wordt gemaakt van de SWIFT-8007-diskette.

Datacom
Voor de aanleveraars via datacom, met BDS-oud en BDS-nieuw, is het mogelijk, naast de controletotalen via een aparte sessie, de integriteit van de betalingsgegevens te beveiligen door een hash-code in het sluitrecord van een SWIFT-batch toe te voegen.
Voor het aanleveren via datacom met BDS-nieuw is het mogelijk ook de authenticiteit van de betalingsgegevens te beveiligen, door behalve de hash-code ook een elektronische handtekening te gebruiken.
Ten slotte kan door middel van lijnencryptie het traject Bank - BGC worden beveiligd, voornamelijk tegen afluisteren.

Al deze mogelijkheden zijn echter optioneel, hetgeen aan de sterkte van de beveiliging van datacom als zodanig afbreuk doet.

Tape/cartridge
De aanleveraars van tapes en cartridges maken uitsluitend gebruik van de beveiliging door middel van controletotalen die via papier aan de BGC worden verstrekt.
De, facultatieve, handtekeningcontrole is een eenvoudige manier van authenticiteitscontrole.
De tape-indeling staat het facultatieve gebruik van een authenticiteitsrecord toe. In dit record staan onder andere een hash-code en een elektronische handtekening.

De toekomstige mogelijkheid van het binnenlandse SWIFT-8007-circuit via DNB

Ontwikkelingen zijn nog gaande en het toekomstige "plaatje" ligt nog niet vast. Vermoedelijk zal in de nieuwe situatie de BGC voornamelijk fungeren als netwerkleverancier. Dit houdt in dat batches die de BGC ontvangt uit het SWIFT-8007-circuit zonder inhoudelijke en syntaxcontrole en zonder controle van authenticiteit en integriteit, wel eventueel na conversie, zullen worden doorgestuurd naar DNB. Hetzelfde geldt voor batches die de BGC van DNB ontvangt en die bestemd zijn voor de deelnemende banken in het door hen verlangde formaat.
Ongewijzigd blijft het beheer door de BGC van de datacomfaciliteiten, tussen banken en de BGC, en van de BGC-PC.

CONCLUSIE

Een vergelijking tussen het door S.W.I.F.T aangeboden netwerk en het binnenlandse SWIFT-8007-circuit levert nogal wat verschillen op. Doordat de banken gebruik kunnen maken van verschillende media in het binnenlandse circuit kunnen zij ook van verschillende beveiligingsmixen gebruik maken. Het is van belang dat de individuele banken bij de keuze van het medium stilstaan bij de mogelijkheden en de onmogelijkheden die door de verschillende wijzen van datatransport worden geboden. De effectiviteit van de beveiliging zal afhangen van de gekozen technische maatregelen en van de organisatorische maatregelen die in de eigen organisatie moeten zijn getroffen. Het resultaat moet in ieder geval de risico's kunnen afdekken die van dit circuit uitgaan.

Drs. F.G. Knaack
Is sedert vier jaar werkzaam bij de afdeling EDP Auditing van de BankGiroCentrale. Daarvoor was hij werkzaam op de ontwikkelafdeling van deze organisatie.

Betrouwbaarheid van het FA-systeem

Drs. R. Oudega

Het betalingscircuit van De Nederlandsche Bank, ook wel topgirocircuit genoemd, is vooral bestemd voor het verrichten van grote betalingen.
Van De Bank als toezichthouder mag worden verwacht dat zij voor het afwikkelen van dergelijk kritisch betalingsverkeer een betrouwbare infrastructuur ter beschikking stelt.
Begin dit jaar is DNB begonnen met de introductie van een vernieuwd systeem, waarvan de beveiligingsmogelijkheden, hoewel nog niet ten volle benut, een voorbeeldfunctie zouden moeten kunnen vervullen.

INLEIDING

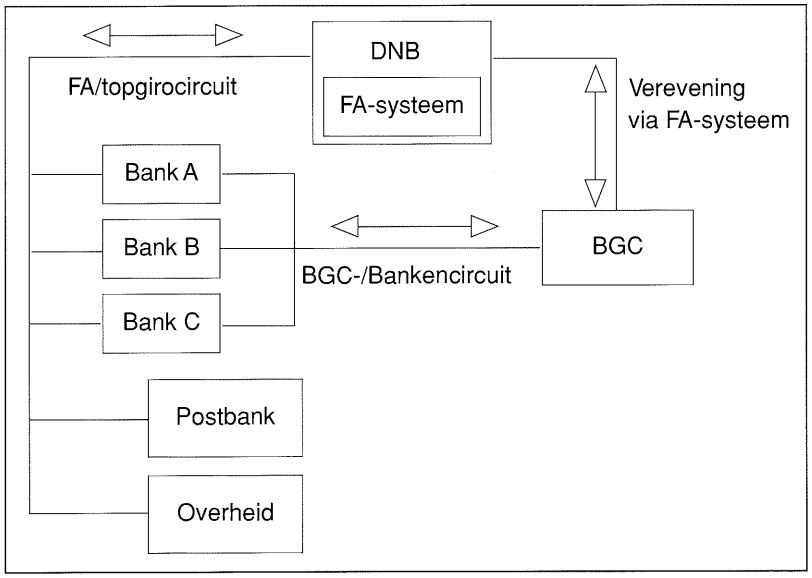
Reeds vanaf het begin van de ontwikkeling van het giraal betalingsverkeer zijn door De Nederlandsche Bank (DNB) clearing-instanties in het leven geroepen voor banken. Deze instanties hielden zich bezig met de verrekening van onder meer het interbancaire betalingsverkeer. Na de oprichting van de BankGiroCentrale door de banken in 1967 werd een deel van de clearing-functie aan DNB onttrokken. Betalingen met gegarandeerde cheques en het merendeel van het overige giroverkeer werden voortaan via de BankGiroCentrale geleid. Wel bleef de verrekening van betalingen tussen rekeninghouders bij DNB onderling uit hoofde van arbitrage, daggelden, telefonische giro-opdrachten en dergelijke een taak van De Nederlandsche Bank.
In 1980 werd de laatste clearing-instantie opgeheven. Door De Nederlandsche Bank was inmiddels een systeem in gebruik genomen waarmee houders van rekeningen bij DNB online giro-opdrachten konden inzenden. Dit systeem is de voorloper van het huidige Financiële Administratiesysteem van De Nederlandsche Bank. In 1992 is het Financiële Administratiesysteem ingrijpend vernieuwd. De verwerking van telefonische giro-opdrachten is door de banken ondergebracht bij de BankGiroCentrale in een apart spoedcircuit.

In dit artikel wordt eerst kort ingegaan op de plaats van het Financiële Administratiesysteem in het betalingsverkeer. Vervolgens worden na een korte beschrijving van de functionaliteit en de benodigde apparatuur de, door DNB getroffen, beheersingsmaatregelen in en rond het Financiële Administratiesysteem beschreven. Bij deze beschrijving is onderscheid gemaakt tussen fysieke, technische (hard- en software-matige) en organisatorische maatregelen.
Geëindigd wordt met het vermelden van enige aandachtspunten voor de situatie dat bij een deelnemer van het Financiële Administratiesysteem, zoals een bank of overheidsinstelling, een onderzoek wordt uitgevoerd naar de betrouwbaarheid en continuïteit van het gebruik van dit betalingscircuit.
Dit artikel betreft het Financiële Administratiesysteem zoals dat door De Nederlandsche Bank eind 1985 is aangeboden aan haar deelnemers en in 1992 ingrijpend is vernieuwd.

ALGEMEEN

Rekeninghouders bij De Nederlandsche Bank nemen deel in het betalingscircuit van DNB, het zogenaamde topgirocircuit, en kunnen betalingen in guldens aan elkaar verrichten door middel van giro-opdrachten. Deze giro-opdrachten kunnen via het deelsysteem rekening-courant van de Financiële Administratie (hierna FA-systeem) aan DNB worden doorgegeven. Ook de verevening van het betalingsverkeer via de BankGiroCentrale (BGC) wordt in het FA-systeem uitgevoerd. De BGC zendt daartoe dagelijks een opdracht aan DNB met de debiteringen en crediteringen van de betrokken banken. Naast het ingeven van giro-opdrachten kunnen de deelnemers via het FA-systeem doorlopend hun positie bij DNB bepalen.
De tendens is slechts grote betalingen via het FA-systeem te leiden en de kleinere bedragen via de BGC af te wikkelen. Dagelijks worden door het FA-systeem drie- à vierduizend giro-opdrachten verwerkt met een gemiddelde omvang van negentien miljoen gulden per opdracht.
Deelnemers aan het FA-systeem zijn:
- banken;
- Postbank;
- BankGiroCentrale;
- ministerie van Financiën;
- rekenplichtigen van de overheid, waaronder de ontvangers der belastingen;
- enkele grote (semi-)overheidsinstellingen;
- andere centrale banken.

De plaats van het FA-systeem in het betalingsverkeer is schematisch weergegeven in figuur 1.



Figuur 1. Plaats FA-systeem in het betalingsverkeer.

FUNCTIONELE BESCHRIJVING FA-SYSTEEM

In deze paragraaf wordt een functionele beschrijving gegeven van de wijze waarop het invoeren en verwerken van giro-opdrachten en guldensmutaties door/via DNB plaatsvindt.

Invoeren en verwerken van giro-opdrachten

Opdrachten worden ingevoerd in een verzamelgiro. Een verzamelgiro heeft per dag of verwerkingsdatum een uniek nummer, dat wordt toegekend door de deelnemer zelf. De invoer van een verzamelgiro (deze kan maximaal dertig opdrachten bevatten) wordt afgesloten met het totaal aantal opdrachten en het totaalbedrag. Onderscheid kan worden gemaakt tussen de volgende soorten giro-opdrachten:
- herroepelijke giro-opdrachten;
- onherroepelijke giro-opdrachten;
- wachtposten.

Aan het eind van een werkdag wordt een dagfiat gegeven. Fiat wordt gegeven voor het totaal aantal verzamelgiro's en het totaal-generaal van de bedragen.

Herroepelijke giro-opdrachten
Een herroepelijke giro-opdracht (ook wel zachte giro-opdracht genoemd) is een opdracht die de gehele periode voor het inbrengen van het dagfiat door de deelnemer kan worden ingetrokken. Herroepelijke giro-opdrachten worden onherroepelijk op het moment dat alle deelnemers hun dagfiat correct hebben ingebracht en DNB heeft vastgesteld dat geen enkele rekening een ontoelaatbare stand vertoont. Voor het opgeven van een herroepelijke giro-opdracht is een minimumbedrag vastgesteld. Bedragen beneden het minimum kunnen alleen als onherroepelijke opdracht worden uitgevoerd.

Onherroepelijke giro-opdrachten
Een onherroepelijke giro-opdracht (ook wel harde giro-opdracht genoemd) is een girale guldensmutatie die na het fiatteren van de bijbehorende verzamelgiro niet meer door de deelnemer kan worden ingetrokken.
Voor de definitieve verwerking van een onherroepelijke verzamelgiro wordt eerst verplicht een invoerverslag aangemaakt.

Wachtposten
Wachtposten zijn herroepelijke giro-opdrachten die kunnen worden ingevoerd met een verwerkingsdatum tot maximaal één maand na de dag van inbreng.

Fiatteren
Eenmaal per dag dient de deelnemer een dagfiat te geven voor de ingebrachte herroepelijke en onherroepelijke verzamelgiro's en voor de op die dag verwerkte verzamelgiro's met wachtposten. Na het ingeven van het dagfiat kan een deelnemer behalve wachtposten geen giro-opdrachten meer invoeren.

Na de eindtijd[1] worden rekeningen met onvoldoende dispositieruimte gemeld bij de DNB-hoofdbank. De desbetreffende deelnemer wordt verzocht een of meer opdrachten in te trekken. DNB kan tevens toestemming verlenen nagekomen posten in te brengen. Indien de dispositieruimte van de deelnemer hierna voldoende is dient hij opnieuw een dagfiat te geven.

Invoeren en verwerken guldensmutaties door/via DNB

De behandeling van guldensmutaties in het FA-systeem is mede afhankelijk van het soort mutatie, hetgeen blijkt uit onderstaande beschrijving.

BGC-verevening
De BGC-vereveningsposten worden als onherroepelijke giro-opdrachten door de BGC ingevoerd. De verevening bestaat uit een verzamelgiro met te debiteren rekeningen en een verzamelgiro met te crediteren rekeningen. Indien een of meer deelnemers aan de verevening over onvoldoende dispositieruimte beschikken wordt bij de BGC en de DNB-hoofdbank een bericht geprint. De vereveningsopdrachten worden geweigerd en de desbetreffende deelnemers wordt verzocht de rekeningen aan te zuiveren, zodat de verevening opnieuw kan worden aangeboden.

Chartale mutaties
Chartale mutaties worden ingevoerd bij bankkantoren van DNB en verwerkt als onherroepelijke mutatie. Chartale mutaties kunnen zijn:

- Cheque-wachtpost. Banken kunnen door middel van cheques beschikken over bankbiljetten. Aangeboden cheques dienen door een bankkantoor van DNB een werkdag voor de dag van overdracht van bankbiljetten te worden ingebracht. Per ingebrachte cheque wordt een blokkade op de rekening aangebracht die de volgende werkdag wordt omgezet in een onherroepelijke debitering.

- Dispositie. Bij kasopname wordt de dispositieruimte gecontroleerd. Indien de dispositieruimte voldoende is wordt deze gemuteerd en wordt bij de deelnemer een debetadvies afgedrukt.

- Stortingen. Na een storting wordt de dispositieruimte gemuteerd. Van de storting wordt bij het inbrengende DNB-bankkantoor een bewijs afgedrukt en bij de houder van de betrokken rekening een creditadvies.

Overige guldensmutaties
Een aantal guldensmutaties wordt door DNB zelf ingevoerd en verwerkt. Deze mutaties betreffen onder meer:
- mutaties uit hoofde van speciale beleningen of van de geldmarkt-kasreserveregeling;
- mutaties uit hoofde van rente en/of kosten;
- opdrachten aangeleverd op tape;
- automatische overboekingen.

Van de verwerkte guldensmutaties worden debet- en creditadviezen afgedrukt bij de desbetreffende deelnemers.

Opvragen

De deelnemers kunnen informatie opvragen over de eigen positie bij DNB, ingevoerde mutaties, toegekende bevoegdheden en chipkaarten, en de eigen configuratie. De informatie kan op het scherm worden geraadpleegd en naar keuze worden afgedrukt op de printer.

Boodschappen versturen

DNB-hoofdbank, DNB-bankkantoren en online aangesloten instellingen kunnen boodschappen naar een of meer online aangesloten deelnemers verzenden. De boodschappen worden bij de ontvangende deelnemer op de hoofdprinter afgedrukt. Het verzenden van boodschappen dient door twee functionarissen te worden uitgevoerd. Deze functie kan onder meer worden gebruikt bij de procedure die wordt toegepast bij het transport van bankbiljetten.

APPARATUUR/DATACOMMUNICATIE

Deelnemen aan het FA-systeem is alleen mogelijk met door DNB beschikbaar gestelde apparatuur en programmatuur. De deelnemende instelling mag en kan de apparatuur niet voor andere toepassingen gebruiken.
De deelnemers hebben via een DN-1 PVC-aansluiting[2] verbinding met DNB. Als uitwijkvoorziening is een SVC-aansluiting gecontracteerd.
De standaardconfiguratie wordt gevormd door de volgende componenten:
- IBM PS/2 model 55 met DOS als besturingssysteem;
- printer, met speciale voorzieningen om verloren gaan/verminken van printberichten te voorkomen;
- modem, communicatiekaart;
- cryptographic adapter, een TSS-component[3] voor cryptografische beveiliging van de transacties;
- persoonsgebonden chipkaarten;
- chipkaartlezer en een TSS-component voor authenticatie van de systeemgebruikers.

De volgende configuraties zijn mogelijk:
- stand-alone-configuratie. Dit is de standaardconfiguratie, eventueel uitgebreid met een extra printer;
- LAN-configuratie. Deze configuratie bestaat uit twee of meer standaardconfiguraties, eventueel uitgebreid met extra printers voor gemeenschappelijk gebruik. Eén PS/2 in het netwerk fungeert tevens als gateway/server naar de centrale computer bij DNB.

Op het werkstation is een diskette-unit aanwezig, die slechts kan worden gebruikt door DNB.

1 *De eindtijd is het tijdstip tot wanneer er online guldensmutaties mogen worden ingevoerd en gefiatteerd. De sluitingstijd is het tijdstip waarop de online werkdag van het FA-systeem wordt afgesloten. Tot de sluitingstijd kunnen opvragingen worden gedaan en/of wachtposten worden ingevoerd.*

2 *Een PVC-aansluiting (Permanent Virtual Circuit) is te vergelijken met een vaste huurlijnverbinding. Een SVC-aansluiting (Switched Virtual Circuit) is vergelijkbaar met een kieslijn.*

3 *TSS staat voor Transaction Security System, een door IBM ontwikkeld systeem voor beveiliging van PC's, communicatie tussen PC's onderling en tussen PC's en host computers.*

BEHEERSINGSMAATREGELEN

Het doel van de beheersingsmaatregelen zoals die in en rond het FA-systeem zijn getroffen, is te waarborgen dat slechts juiste en geautoriseerde betalingen worden uitgevoerd.

Navolgend is een beschrijving opgenomen van de getroffen beheersingsmaatregelen, waarbij onderscheid is gemaakt tussen fysieke, technische en organisatorische maatregelen. De technische maatregelen omvatten maatregelen op het gebied van hard- en software.
Vervolgens wordt nader ingegaan op de maatregelen die een betrouwbare invoer en verwerking van de giro-opdrachten ondersteunen en de continuïteit waarborgen.

Fysieke maatregelen

De besturingseenheid van de werkstations is ingebouwd in een stalen kast, voorzien van een contactslot voor het aan- en uitschakelen van de netspanning. De kast is voorzien van twee sloten, een voor de deelnemende instelling en een onder beheer van de firma die namens DNB het onderhoud verzorgt en technische storingen verhelpt. De kast beschermt tegen ongeautoriseerd verwijderen van de Cryptographic Adaptor en tegen ongeautoriseerd gebruik van het diskettestation (laden van andere dan door DNB geïnstalleerde programmatuur).
Het diskettestation kan niet worden gebruikt voor andere toepassingen en is voorzien van twee sloten. De sleutels daarvan zijn onder beheer van DNB.

Technische maatregelen

De maatregelen die zijn getroffen in de hard- en software betreffen:
- authenticatie van programmatuur op de werkstations;
- identificatie/authenticatie;
- autorisatie;
- encryptie.

Hierna zijn deze maatregelen nader toegelicht, waarbij - indien van toepassing - onderscheid wordt gemaakt tussen een deelnemer (een instelling) en een systeemgebruiker (een natuurlijk persoon).

Authenticatie van programmatuur op de werkstations
Per bestand (inclusief de programmatuur) is een hash count gemaakt, die encrypt is opgeslagen. Bij het opstarten van de werkstations wordt per bestand de hash count opnieuw berekend en vergeleken met de opgeslagen hash count. Indien verschillen worden geconstateerd, wordt daarvan melding gemaakt en wordt de deelnemer geadviseerd contact op te nemen met de Supervisor-giro van DNB. Indien geen maatregelen worden getroffen, kan het werkstation de volgende dag niet worden gebruikt.

Identificatie/authenticatie
Voor de identificatie en authenticatie van een deelnemer en systeemgebruikers wordt gebruik gemaakt van chipkaarten, een deelnemernummer, administratienummers en passwords. Voor de aanmelding van een deelnemer wordt na het inbrengen van de chipkaart verbinding gelegd met de centrale computer om toegang te krijgen tot de FA-functies. Een bevoegde systeemgebruiker meldt de deelnemer aan door het deelnemernummer, het eigen administratienummer en het password in te toetsen. Na controle op de autorisatie van de deelnemer en de systeemgebruiker wordt bij akkoord het scherm "Aanmelden terminalbediende" ter beschikking gesteld.
Systeemgebruikers kunnen aanloggen op het FA-systeem door de persoonlijke chipkaart in te brengen in de chipkaartlezer en het administratienummer en het password in te voeren. Het FA-systeem controleert:
- of het administratienummer voorkomt bij de deelnemer;
- of het administratienummer behoort bij de chipkaart;
- of het password behoort bij het administratienummer.

Het doel van de beheersingsmaatregelen zoals die in en rond het FA-systeem zijn getroffen, is te waarborgen dat slechts juiste en geautoriseerde betalingen worden uitgevoerd.

Indien deze identificatiecontroles niet tot foutmeldingen leiden, worden de systeemgebruiker de laatste datum en tijd van aanmelding gegeven. Na verificatie door de systeemgebruiker wordt het keuzemenu ter beschikking gesteld.

Na zes foutieve aanlogpogingen worden de gegevens van de desbetreffende systeemgebruiker verwijderd. Indien de combinatie administratienummer/chipkaartnummer onjuist is, worden na zes foutieve pogingen tevens de gegevens behorende bij het chipkaartnummer verwijderd. Van de verwijderingen wordt zowel bij de deelnemer als bij de DNB-hoofdbank een verslag geprint.

Een systeemgebruiker heeft een persoonlijk password en kan dit zonder tussenkomst van anderen wijzigen. Het systeem registreert de datum en tijd van de laatste wijziging. Wekelijks wordt door het FA-systeem gecontroleerd of de systeemgebruikers recentelijk hun password hebben gewijzigd en gebruik hebben gemaakt van het systeem. Bij deze controle worden drie gevallen onderscheiden:

- Indien het FA-systeem bij het aanloggen signaleert dat de systeemgebruiker meer dan 14, maar

minder dan 22 dagen geen gebruik heeft gemaakt van het FA-systeem, wordt de systeemgebruiker gedwongen zijn password te wijzigen.

– Het password is meer dan 21, maar minder dan 43 dagen niet gewijzigd. Van de systeemgebruiker wordt de aanlogbevoegdheid verwijderd. Na hernieuwd toekennen van de aanlogbevoegdheid van de systeemgebruiker door de security-functionarissen dient de gebruiker eerst zijn password te wijzigen.

– Het password is meer dan 42 dagen niet gewijzigd. Het administratienummer, de bijbehorende bevoegdheden en het chipkaartnummer worden uit het FA-systeem verwijderd.

Binnen de organisatie van de deelnemer kan controle worden uitgeoefend op het regelmatig wijzigen van passwords door het overzicht van administratienummers op te vragen. Op dit overzicht is per administratienummer de datum van de laatste password-wijziging opgenomen.

Door DNB wordt aan de deelnemers een aantal chipkaarten uitgereikt. Iedere chipkaart heeft een uniek nummer, dat tevens is vastgelegd bij de deelnemergegevens in het FA-systeem. Zodra een systeemgebruiker bekend wordt gemaakt in het FA-systeem ontvangt hij een chipkaart, die vervolgens door twee functionarissen aan het administratienummer wordt gerelateerd.

Een chipkaart wordt automatisch ongeldig verklaard na zes foutieve aanlogpogingen van een systeemgebruiker. Daarnaast heeft het systeem een functie waarmee chipkaarten ongeldig kunnen worden verklaard in geval van verlies, beschadiging of diefstal. Ongeldig verklaarde chipkaarten dienen te worden verzonden naar DNB, waar de chipkaarten geschikt worden gemaakt voor hergebruik.

Bij het aanloggen van systeemgebruikers op het FA-systeem wordt gebruik gemaakt van een Message Authentication Code (MAC)[4]. Met behulp van een MAC kan de integriteit van een bericht worden vastgesteld.
Voorlopig wordt alleen gebruik gemaakt van een MAC bij het aanloggen. In de toekomst zal ook aan de overige berichten een MAC worden toegevoegd.

Autorisatie
Afhankelijk van de benodigde functies zijn deelnemers verdeeld in een aantal soorten. Per soort deelnemer wordt een aantal functies toegekend. De verschillende soorten deelnemers zijn:
- ministerie van Financiën;
- BankGiroCentrale. De BGC heeft als enige deelnemer de bevoegdheid andere dan de eigen rekeningen te debiteren. Deze bevoegdheid is noodzakelijk voor het uitvoeren van de verevening;
- administratiegroep Chartaal betalingsverkeer, een afdeling binnen DNB;
- niet-bancaire rekeninghouders;
- bancaire rekeninghouders.

In deze beschrijving komen met name die functies aan de orde die van belang zijn voor de bancaire en niet-bancaire rekeninghouders.

De functies die ter beschikking staan van de deelnemer kunnen worden verdeeld over de systeemgebruikers. Uit het oogpunt van functiescheiding is een aantal combinaties van functies niet toegestaan (zie tabel 1).

Bij de invoer en het onderhoud van bevoegdheden per systeemgebruiker controleert het FA-systeem of voornoemde combinaties van bevoegdheden zijn toegekend. Indien deze combinaties zijn toegekend, worden deze door het FA-systeem geweigerd.
De invoer en het onderhoud van systeemgebruikers en bevoegdheden vormen samen een functie die door twee functionarissen dient te worden uitgevoerd. Controle van de bevoegdheden kan worden uitgevoerd door deze op te vragen op het scherm en aan de hand van een wekelijks overzicht van DNB.

Om ongeautoriseerd gebruik van het werkstation tegen te gaan bij afwezigheid van de systeemgebruiker wordt gebruik gemaakt van een time out-mechanisme. Indien een systeemgebruiker vijf minuten geen gebruik heeft gemaakt van het FA-systeem wordt de gebruiker gevraagd het password opnieuw in te voeren. Het ingevoerde password wordt vergeleken met het password dat bij het aanloggen voor dit doel op de chipkaart is vastgelegd. Als er niet binnen 25 minuten wordt gereageerd op dit verzoek, wordt de FA-sessie afgebroken. De gebruiker dient daarna, indien hij opnieuw gebruik wil maken van het FA-systeem, opnieuw de chipkaart in te voeren en aan te loggen.

Encryptie
Het berichtenverkeer tussen het FA-systeem en de werkstations is vercijferd (encrypt) volgens het DES-algoritme[5].

Organisatorische maatregelen

Om te waarborgen dat slechts geautoriseerde apparatuur en programmatuur wordt gebruikt door de deelnemer worden de configuratie en de software door DNB geïnstalleerd. Onderhoud van de apparatuur wordt namens DNB uitgevoerd door een door DNB aangewezen instantie.

Bij vragen en problemen kunnen de deelnemers contact opnemen met de Supervisor-giro, de door DNB aangestelde beheerder van het FA-systeem die een begeleidende en coördinerende rol heeft.
Iedere deelnemer heeft een interne-controlefunctionaris die optreedt als contactpersoon naar DNB. Bijzondere gebeurtenissen worden door DNB aan deze functionaris gemeld. Voorbeelden van bijzondere gebeurtenissen zijn:
- tijdelijk toekennen van een extra administratienummer;
- verwijderen van administratienummers en/of ongeldig maken van chipkaarten na foutieve aanlogpogingen.

4 Aan een bericht wordt een code toegevoegd (MAC1) die wordt berekend uit het bericht zelf en een geheime sleutel. De ontvanger van het bericht berekent de code opnieuw (MAC2) met dezelfde geheime sleutel en het ontvangen bericht. Indien tijdens het verzenden wijzigingen in het bericht optreden zal de uit het ontvangen bericht herberekende code (MAC2) verschillen van de meegezonden code (MAC1).
Voor het berekenen van de MAC wordt een sleutel gebruikt, die uniek is per administratienummer. De cryptografische sleutel ten behoeve van de MAC-berekening is in de persoonlijke chipkaart opgeslagen.

5 Encryptie van een bericht is een techniek waarbij de zender het bericht volgens een bepaald algoritme, gebruik makend van een geheime sleutel, vercijfert. De ontvanger kent het algoritme en de geheime sleutel en kan het vercijferde bericht terug vercijferen naar het originele bericht. Voor encryptie van gegevens zijn meerdere algoritmen beschikbaar. Data Encryption Standard, of DES, is daarvan momenteel het meest gebruikte.
Het FA-systeem maakt gebruik van een standaard-encryptiefaciliteit van IBM (SNA-sessie-encryptie). Dagelijks wordt per deelnemer een nieuwe sleutel gebruikt.

Maatregelen invoeren en verwerken giro-opdrachten

Bij de invoer van giro-opdrachten door deelnemers worden geautomatiseerde controles uitgevoerd door het FA-systeem die de juistheid en de volledigheid van de giro-opdrachten ondersteunen. Tevens worden per toepassing na invoer en verwerking verslagen afgedrukt bij de betrokken deelnemers en DNB. Onderstaand is beschreven welke maatregelen bij de verschillende functies zijn getroffen ten aanzien van de invoer en verwerking.

Giro-opdrachten
De invoer van giro-opdrachten in een verzamelgiro wordt afgesloten met het totaal van het aantal posten en het totaalbedrag. De ingevoerde totalen van de verzamelgiro worden vergeleken met de door het FA-systeem opgebouwde totalen. Indien de totalen overeenstemmen is verdere verwerking mogelijk. Stemmen zij niet overeen, dan wordt de verzamelgiro als onafgesloten beschouwd en is verdere verwerking pas weer mogelijk na invoer van de juiste totalen.
De te crediteren rekeningnummers dienen bekend te zijn binnen het FA-systeem.
Voor de verschillende soorten giro-opdrachten zijn verder verschillende maatregelen getroffen. Deze worden hierna gegeven.

Na het afsluiten van een verzamelgiro met herroepelijke giro-opdrachten worden bij de betrokken deelnemers debet- en creditberichten afgedrukt. De debet- en creditberichten zijn apart oplopend genummerd. Bij de inbrengende deelnemer wordt tevens een verzamelgirobericht afgedrukt.

Nadat een verzamelgiro met wachtposten is afgesloten, wordt bij de inbrengende deelnemer een verzamelgirobericht afgedrukt. Op de verwerkingsdatum van de verzamelgiro worden de wachtposten als herroepelijke giro-opdrachten verwerkt. Bij de betrokken deelnemers worden debet- en creditberichten afgedrukt.

Na het afsluiten van een verzamelgiro met onherroepelijke giro-opdrachten worden een invoerverslag en een voorlopig verzamelgirobericht afgedrukt. Het invoerverslag bevat een printnummer. Het printnummer is een uniek nummer binnen een werkdag dat aan een printboodschap wordt gegeven door het centrale systeem. De verzamelgiro kan worden gecontroleerd op juistheid en volledigheid aan de hand van het invoerverslag, het verzamelgirobericht en de brondocumenten. Indien deze controle leidt tot correcties wordt na het afsluiten van de verzamelgiro opnieuw een invoerverslag afgedrukt. Na controle dient de verzamelgiro te worden gefiatteerd door een andere systeemgebruiker. Bij het fiatteren worden het totaal aantal posten, het totaal van de bedragen en het printnummer van het laatste invoerverslag van de verzamelgiro ingevoerd. De ingevoerde totalen van de verzamelgiro worden vergeleken met de door het FA-systeem opgebouwde totalen en de juistheid van het printnummer wordt vastgesteld. Indien de totalen overeenstemmen wordt door het FA-systeem de dispositieruimte berekend. Bij onvoldoende ruimte behoudt de verzamelgiro de status voorlopig. Bij voldoende ruimte wordt de verzamelgiro verwerkt. Bij de betrokken deelnemers en bij DNB-hoofdbank worden debet- en creditopgaven afgedrukt. Bij de inbrengende deelnemer wordt tevens een verzamelgirobericht afgedrukt.
Indien de fiattotalen niet overeenstemmen wordt de verzamelgiro niet verwerkt en blijft deze als voorlopig gekenmerkt. Het is niet mogelijk meer dan vijf ongefiatteerde verzamelgiro's in te voeren.

Functie	Onverenigbaar met functie:
Toevoegen van administratienummers en bevoegdheden	Invoeren en corrigeren giro-opdrachten
Invoeren en corrigeren herroepelijke opdrachten	Inbrengen fiatteringstotalen dagfiat
Invoeren en corrigeren wachtposten	Inbrengen fiatteringstotalen dagfiat
Invoeren en corrigeren onherroepelijke opdrachten	Fiattering harde verzamelgiro en inbrengen fiatteringstotalen dagfiat
Intrekken giro-opdrachten	Inbrengen fiatteringstotalen dagfiat

Tabel 1. Niet-toegestane combinaties van functies.

Guldensmutaties door DNB
Van mutaties die door DNB zijn uitgevoerd, worden debet- en/of creditberichten afgedrukt bij de betrokken deelnemers.

Correcties
Verwerkte herroepelijke verzamelgiro's kunnen worden ingetrokken voor het dagfiat is ingegeven. Na het intrekken van giro-opdrachten worden bij de betrokken deelnemers intrekkingsberichten afgedrukt.

Chartale mutaties kunnen op verzoek van het inbrengende DNB-bankkantoor door DNB-hoofdbank worden ingetrokken. Van de intrekking wordt een bericht afgedrukt bij de deelnemer, het inbrengende DNB-bankkantoor en DNB-hoofdbank.

Fiatteren
Het dagfiat wordt gegeven door het totaal aantal afgesloten verzamelgiro's (inclusief de op die dag verwerkte verzamelgiro's met wachtposten) en het totaal van de opdrachten in te voeren. Het FA-systeem vergelijkt de ingevoerde totalen met de totalen die door het FA-systeem zelf zijn opgebouwd

bij verwerking van de verzamelgiro's. Indien een verschil wordt geconstateerd, wordt dit op het scherm gemeld. De deelnemer dient vervolgens zelf aan de hand van brondocumenten de totalen te herberekenen.

Het FA-systeem vergelijkt de ingevoerde totalen met de totalen die door het FA-systeem zelf zijn opgebouwd.

De fiattotalen kunnen tussentijds worden gecontroleerd met de functie "Inbrengen controletotaal dagfiat". Deze functie geeft na invoer van de fiattotalen de melding akkoord of niet akkoord.

Maatregelen continuïteit

De maatregelen met betrekking tot de continuïteit vallen uiteen in die ten aanzien van de totale configuratie en die ten aanzien van de centrale configuratie en de datacommunicatie.

Maatregelen lokale configuratie
Periodiek onderhoud en het oplossen van storingen worden uitgevoerd door een firma die gespecialiseerd is op dat gebied. In geval van storing dient de deelnemer contact op te nemen met de Supervisor-giro. Naast de functie van Supervisor-giro heeft DNB tevens een Helpdesk ingesteld.

Indien zich een printerstoring voordoet bij een deelnemer kan de Supervisor-giro de logische koppeling tussen een werkstation en een bijbehorende printer real time wijzigen. De printberichten worden tevens opgeslagen in het FA-systeem. Niet bij de deelnemer afgedrukte printberichten worden dagelijks na sluitingstijd afgedrukt bij DNB-hoofdbank en kunnen op verzoek aan de deelnemer worden verzonden.

Maatregelen centrale configuratie/datacommunicatie
In geval van ernstige storing van het centrale FA-systeem worden de deelnemers door de Supervisor-giro ingelicht omtrent de verwachte duur van de storing. De deelnemers kunnen aan de hand van de verwachte storingsduur bepalen of zij al dan niet opdrachten op een alternatieve wijze gaan aanleveren. Alternatieve manieren om de opdrachten aan te leveren zijn:
- schriftelijke opdrachten inleveren bij één van de DNB-kantoren;
- opdrachten aanleveren op tape;
- aanleveren van opdrachten bij DNB onder code per telefoon, fax of telex. Dit alternatief is slechts mogelijk voor instellingen die individueel met DNB een code-uitwisselingsprocedure zijn overeengekomen.

Indien interne uitwijk bij DNB niet mogelijk is, kan bij belangrijke verstoring van de continuïteit van de centrale computer bij DNB worden uitgeweken naar het ComputerUitwijkCentrum (CUC). De deelnemers kunnen aanloggen op het FA-systeem door op te starten met behulp van een speciale chipkaart, waarna gekozen kan worden voor de uitwijkverbinding.

Nadat de storing bij DNB is verholpen, wordt bepaald in hoeverre mutaties verloren zijn gegaan, waarna de Supervisor-giro de deelnemers zal meedelen tot welk tijdstip mutaties zijn verwerkt. Na het bericht van de Supervisor-giro wordt de verbinding weer opengesteld.

AUDITING-ASPECTEN

De maatregelen die door DNB zijn getroffen in en rond het FA-systeem dienen te worden aangevuld door de organisatie die het FA-systeem gebruikt (de deelnemer). Deze aanvullingen betreffen organisatorische en fysieke maatregelen. De organisatorische maatregelen dienen ervoor zorg te dragen dat op een juiste manier gebruik wordt gemaakt van de door het FA-systeem geboden faciliteiten. Met name de implementatie van bevoegdheden en de beheersing daarvan bepalen in hoeverre een betrouwbare invoer en verwerking van opdrachten kan worden gerealiseerd. Ook de behandeling van de overzichten en de reconciliatieprocedures zijn daarbij van groot belang.
De fysieke maatregelen dienen erop gericht te zijn de FA-configuratie verder af te schermen.

Bij een onderzoek naar de betrouwbaarheid en continuïteit van het gebruik van het FA-systeem bij een deelnemer dient de auditor zich het volgende te realiseren:

- Topgirocircuit. Het topgirocircuit kent slechts een beperkt aantal deelnemers en rekeningen; daardoor is het risico dat bedragen niet bij de juiste begunstigde terecht komen beperkt.

- Functiescheiding. Het FA-systeem dwingt een beperkte mate van functiescheiding af. Voor het uitvoeren van giro-opdrachten zijn twee functionarissen noodzakelijk. Het grootste risico doet zich voor bij de invoer en verwerking van herroepelijke betalingsopdrachten. Deze opdrachten kunnen door één functionaris worden ingevoerd en verwerkt. Voor het invoeren van het dagfiat, waardoor de herroepelijke opdrachten onherroepelijk worden, is controle van deze opdrachten van groot belang.

De deelnemer heeft wel de mogelijkheid de bevoegdheid per functionaris verder te beperken.

- Datacommunicatie. Bij het aanloggen wordt gebruik gemaakt van een Message Authentication Code (MAC). Door het toevoegen van een MAC aan een bericht kan de integriteit van dat bericht worden gewaarborgd. Bij het transactieberichtenverkeer wordt (nog) geen gebruik gemaakt van een

MAC. Deze berichten worden versleuteld (encrypt) volgens het DES-algoritme. Encryptie is een beveiliging tegen ongewenst kennisnemen van berichtenverkeer, maar biedt geen honderd procent beveiliging tegen wijziging van de berichten.

– Dagfiat. De fiattotalen die bij het geven van een dagfiat dienen te worden ingevoerd, zijn het totaal aantal verzamelgiro's en het totaal bedrag. Verschuivingen van bedragen van de ene begunstigde naar de andere worden daarmee niet opgemerkt.

TOT SLOT

In dit artikel is na een korte functionele beschrijving nader ingegaan op de beheersingsmaatregelen zoals die in en rond het Financieel Administratiesysteem zijn getroffen door De Nederlandsche Bank. Het FA-systeem is bestemd voor het verrichten van grote betalingen. Voor de afwikkeling van dergelijk kritisch betalingsverkeer dient een betrouwbare infrastructuur aan de deelnemers ter beschikking te worden gesteld.

In 1992 is DNB begonnen met het installeren van het sterk vernieuwde FA-systeem bij de deelnemers. Met dit systeem worden aan de deelnemers ruime mogelijkheden geboden een betrouwbaar betalingsverkeer te realiseren. Daarbij zijn de door de deelnemer getroffen maatregelen van groot belang. Organisatorische en fysieke maatregelen dienen ervoor zorg te dragen dat op een juiste wijze gebruik wordt gemaakt van de geboden faciliteiten.

Verbetering in de geboden infrastructuur kan nog optreden wanneer ook het berichtenverkeer inzake de giro-opdrachten wordt voorzien van een MAC, waardoor de integriteit van deze berichten kan worden gewaarborgd. Hiervoor zijn reeds plannen gemaakt door De Nederlandsche Bank.

Drs. R. Oudega
Is sinds 1990 werkzaam bij KPMG Klynveld EDP Auditors. Hij is bijna afgestudeerd aan de postdoctorale opleiding EDP-auditing aan de Erasmus Universiteit Rotterdam. Bij KPMG Klynveld EDP Auditors maakt hij onder meer deel uit van een research-groep banken en betalingsverkeer en is hij betrokken bij het maken van cursussen hierover.

Een Nederlandse standaard voor de elektronische handtekening

Mw. drs. M.C. van Lith

De auteur van dit artikel is betrokken geweest bij de ontwikkeling van de Nederlandse standaard voor de elektronische handtekening.
In dit artikel zet zij de werking en functionaliteit van de elektronische handtekening op heldere wijze uiteen en gaat zij in op enkele interessante organisatorische en operationele aspecten.

INLEIDING

Om te kunnen vaststellen dat een elektronische betaalopdracht de bank ongewijzigd heeft bereikt en om tevens te kunnen vaststellen dat het een betaalopdracht betreft van een bevoegde relatie, kan gebruik worden gemaakt van een "elektronische handtekening".[1] Een elektronische handtekening kan worden voorgesteld als een bitpatroon met een lengte van tussen de 64 en 1024 bits. De elektronische handtekening wordt berekend op basis van te tekenen data en een persoonsgebonden geheime sleutel.[2]

Om te voorkomen dat de verschillende banken in Nederland elk een eigen methode voor het plaatsen van een elektronische handtekening zouden ontwikkelen, besloot de Commissie Informatiebeveiliging van de Nederlandse Vereniging van Banken (NVB) een voorstel te ontwikkelen voor een standaard voor de elektronische handtekening. Om tot dit voorstel te komen zijn de afgevaardigden van de banken rond de tafel gaan zitten om de voor- en nadelen van de verschillende methoden te bespreken. Als onafhankelijke deskundige op dit terrein werd KPMG Management Consultants uitgenodigd.

Rond het ontwikkelen van de standaard speelde een groot aantal factoren een rol. Voor ieder van die factoren moest een weloverwogen keuze worden gemaakt tussen enerzijds een eenduidige richting inslaan en anderzijds vrijheden openlaten voor eventuele toekomstige nieuwe implementaties, om aldus een praktische standaard op te leveren, waarmee een zo groot mogelijk publiek uit de voeten kan.

Dit artikel richt zich voornamelijk op de functionaliteit en de opbouw van de elektronische handtekening. Daarnaast wordt kort aandacht besteed aan de implementatie in de organisatie en wordt de noodzaak tot karaktersettranslatie en karakterrepresentatie beschreven.

ELEKTRONISCHE HANDTEKENING

"Vroeger" werden financiële transacties "beveiligd" met een handtekening. Het ligt dus voor de hand om elektronische transacties te beveiligen met een elektronische handtekening.

Wat is een elektronische handtekening?

Om te beginnen dient de elektronische handtekening de "ouderwetse" handmatige handtekening te kunnen vervangen. Aan de handtekening dient dus bewijskracht te kunnen worden ontleend ten aanzien van de persoonsidentificatie en de bepaling van de echtheid van de transactie. De elektronische handtekening dient persoonlijk te zijn. De elektronische handtekening dient niet door een ongeautoriseerde persoon te kunnen worden nagemaakt en dient eenduidig verbonden te zijn met de getekende data.

Omdat cryptografie een techniek is die het praktisch onmogelijk maakt data onopgemerkt te veranderen, mits de sleutel geheim wordt gehouden, is cryptografie tevens zeer geschikt voor het berekenen van de elektronische handtekening. Public key-algoritmen[3] lenen zich het best voor het plaatsen van een elektronische handtekening vanwege het asymmetrische karakter van de cryptografische sleutels. De sleutels voor generatie en verificatie van de handtekening zijn in geval van een asymmetrisch algoritme verschillend. Op deze manier wordt non-repudiation[4] verkregen, omdat zender en ontvanger zich niet kunnen voordoen als de ander.

Indien toch gekozen wordt een symmetrisch algoritme te gebruiken voor het genereren van de elektronische handtekening, zijn aanvullende maatregelen vereist voor het verkrijgen van non-repudiation, want zowel zender als ontvanger beschikt over dezelfde cryptografische sleutel.

Public key-algoritmen zijn relatief traag. Om deze reden wordt de handtekening niet over het gehele te beveiligen bericht geplaatst maar wordt eerst een hash-code berekend. Over de aldus verkregen gecomprimeerde data wordt vervolgens de handtekening gezet. De hash-functie[5] dient dusdanig te zijn dat het zeer moeilijk is andere data te construeren resulterend in dezelfde hash-waarde.

Een elektronische handtekening gebaseerd op een goed cryptografisch algoritme is minder gemakkelijk te vervalsen dan een handmatige handtekening. Er dienen echter wel voorzieningen te worden getroffen voor het key management[6]. Slecht sleutelbeheer kan leiden tot compromittering van de sleutels en handtekeningvervalsing.

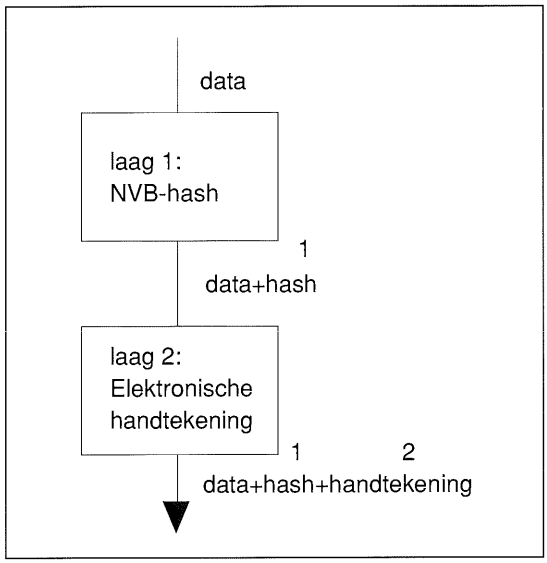
Uit de jurisprudentie komt naar voren dat de bewijskracht van de elektronische handtekening is gebaseerd op contractuele vastleggingen tussen de betrokken partijen. Voorwaarden voor een betrouwbare verwerking zijn dus: een sterk cryptografisch algoritme, een juiste implementatie en een degelijk contract.

End-to-end-beveiliging

Een elektronische handtekening heeft net als een handmatige handtekening een persoonlijk karakter. De handtekening dient eenduidig te zijn terug te leiden tot één persoon of één organisatie. Om deze reden is het ondenkbaar dat bij datacommunicatie de handtekening in een knooppunt wordt vervangen door een handtekening van het knooppunt, door na controle van de oude handtekening een nieuwe handtekening te genereren op basis van een sleutel van het knooppunt. De handtekening verliest hierdoor haar bewijskracht. De elektronische handtekening wordt altijd end-to-end[7] toegepast.

Elektronische handtekening in twee lagen

Voor het genereren van de elektronische handtekening kan gebruik worden gemaakt van het tweelagenprincipe. Alvorens data te tekenen met een elektronische handtekening (laag 2), wordt de data gecomprimeerd door middel van een hash-functie (NVB-hash, laag 1).



Figuur 1. Het twee-lagenprincipe.

De NVB-hash is een op DES[8] gebaseerd gestandaardiseerd algoritme voor de berekening van een controlegetal. De uitkomst van de bewerking is een condensatie van data naar slechts enkele bytes. Bij de berekening van de hash wordt geen gebruik gemaakt van geheime cryptografische sleutels, bovendien is het algoritme voor een ieder toegankelijk. Het controlegetal is daarom niet beschermd tegen het aanbrengen van wijzigingen door onbevoegden.

Om de NVB-hash als integriteitskenmerk[9] te kunnen gebruiken zijn derhalve aanvullende maatregelen noodzakelijk. De elektronische handtekening in de vorm van het integriteitskenmerk vormt hiervoor een goede oplossing. Laag 2, het authentici-

1 Elektronische handtekening: gegevens behorende bij of een cryptografische omzetting van data die een ontvanger in staat stelt de oorsprong en de integriteit van de data te bewijzen en die bescherming biedt tegen vervalsing.

2 Cryptografische sleutel: een opeenvolging van symbolen die de vercijferings- en de ontcijferingsoperatie besturen (ISO DIS 7498-2 Security Architecture).

3 Public key: de sleutel die in een public key-systeem algemeen bekend is (CCITT X.509/ISO 9594-8 Authentication framework).

4 Non-repudiation van de oorsprong: met deze beveiligingsfunctie verkrijgt de ontvanger van een bericht het onweerlegbaar bewijs over de oorsprong van het bericht. Dit zal beschermen tegen elke poging door de verzender om naderhand het bericht of zijn inhoud te herroepen.

5 Hash-functie: een cryptografische functie met als invoer een gegevensreeks van variabele lengte en als resultaat een uitvoer van vaste lengte en met de eigenschap dat het extreem moeilijk is twee verschillende teksten te bepalen die hetzelfde hash-resultaat opleveren.

6 Key management: de generatie, opslag, veilige distributie en toepassing van sleutels in overeenstemming met het beveiligingsbeleid (ISO DIS 7498-2 Security architecture).

7 End-to-end-beveiliging: de beveiliging die door een organisatie wordt verschaft en waar een andere organisatie op vertrouwt (MD4 - Beveiligingsgroep).

8 DES: Data Encryption Standard. Een symmetrisch algoritme. Referentie: ANSI X.3.92, 1981, Data Encryption Algorithm (DEA) en FIPS PUB 46-1, 1988, Data Encryption Standard (DES).

9 Integriteit: de eigenschap dat gegevens niet zijn gewijzigd, toegevoegd of verwijderd.

teitskenmerk, wordt berekend over laag 1, het integriteitskenmerk.

Het authenticiteitskenmerk (de elektronische handtekening) wordt beschouwd als een controlegetal op sublaag 2. Het controlegetal op sublaag 1, de NVB-hash, heeft als doel de integriteit van data te waarborgen. Het authenticiteitskenmerk beschermt het integriteitskenmerk tegen het aanbrengen van wijzigingen en vormt tevens het bewijs voor de authenticiteit van de zender.

DE FUNCTIONALITEIT VAN DE ELEKTRONISCHE HANDTEKENING

De elektronische handtekening heeft twee functies:
- bewaring van de integriteit van de getekende data;
- het authenticeren van de persoon die de data getekend heeft.

Naast deze twee basisfuncties is er een aantal gerelateerde beveiligingsfuncties waarop de elektronische handtekening invloed heeft:
- integriteit van de berichtvolgorde;
- non-repudiation;
- vertrouwelijkheid.[10]

In het vervolg van deze paragraaf worden deze beveiligingsfuncties besproken.

Data-integriteit is een functie die de ouderwetse handtekening niet kende.

Data-integriteit

Data-integriteit is een functie die de ouderwetse handtekening niet kende. Het was mogelijk op blanco passages in een tekst regels toe te voegen. De elektronische handtekening biedt wel bescherming tegen dit soort manipulaties.
De integriteit van de te beveiligen data wordt gewaarborgd door de integriteit van de hash H. De integriteit van H wordt vervolgens gewaarborgd door de elektronische handtekening ES.

H = H(data)
ES = E_k(H) (symmetrisch)
of: ES = D_{sk}(H) (public key)

Voor public key-algoritmen wordt de secret key[11] gebruikt voor de berekening van de elektronische handtekening, voor symmetrische algoritmen de gemeenschappelijke sleutel. Verzonden wordt data // H // ES (de concatenatie van de data, de hash en de elektronische handtekening).

ES wordt gecontroleerd door de ontvanger. Voor handtekeningen op basis van een public key-algoritme is de verificatie anders dan voor handtekeningen op basis van een symmetrisch algoritme. Bij een public key-algoritme wordt de ontvangen elektronische handtekening ES' ontcijferd met de public key, resulterend in de hash H'. Vervolgens wordt de hash H'' opnieuw uit de ontvangen data (data') berekend en wordt het resultaat vergeleken met de uit ES' berekende waarde H'.

$$E_{pk}(ES') = H' =?= H'' = H(data')$$

Als de waarden gelijk zijn, is de handtekening berekend op basis van de juiste geheime sleutel. Aangenomen dat de zender deze geheime sleutel zelf heeft gegenereerd en aan niemand heeft bekend gemaakt, kan worden geconcludeerd dat de ontvangen data integer is.

Als een symmetrisch algoritme wordt gebruikt, dan wordt zowel de hash als de handtekening opnieuw berekend op basis van de gemeenschappelijke sleutel. Het resultaat wordt vergeleken met de ontvangen waarde van de handtekening.

$$ES' =?= ES'' = E_k(H(data'))$$

Als de waarden gelijk zijn, is eveneens de handtekening berekend op basis van de juiste sleutel. Deze sleutel is echter in het bezit van minstens twee partijen (de zender en de ontvanger).

Authenticiteit van de zender

De authenticiteit van de zender is gebaseerd op het bezit van de juiste cryptografische sleutel en kan dus worden aangetoond op basis van de juistheid van de handtekening. Als gebruik wordt gemaakt van een public key-algoritme en als de zender de geheime sleutel zelf heeft gegenereerd en aan niemand bekend heeft gemaakt, kan worden geconcludeerd dat de data inderdaad van de geautoriseerde persoon afkomstig is.
Voor een symmetrisch algoritme is het aantonen van de authenticiteit van de zender lastiger. De ontvanger van het bericht beschikt over dezelfde sleutel en is in staat de berichten zelf te genereren en te tekenen met de gemeenschappelijke sleutel. Afhankelijk van het ermee gemoeide risico, het wederzijdse vertrouwen en eventuele aanvullende maatregelen kan het gebruik van een symmetrisch algoritme niettemin een bevredigend alternatief zijn.

Integriteit van de berichtvolgorde

Door het genereren van een elektronische handtekening is het onmogelijk om een bericht onopgemerkt te wijzigen of toe te voegen, maar er kan niet worden voorkomen dat een bericht onopgemerkt wordt verwijderd of dat een bericht wordt herhaald. Om dergelijke ingrepen te voorkomen zijn aanvullende maatregelen vereist. Met behulp van in de berichten opgenomen volgnummers kan worden vastgesteld of een bericht ontbreekt of dat een bericht is herhaald.

10 Vertrouwelijkheid: de eigenschap dat informatie niet beschikbaar komt of wordt onthuld aan onbevoegde personen, eenheden of processen (ISO DIS 7498-2 Security architecture).
11 Secret key (geheime sleutel): de sleutel die in een public key-systeem geheim gehouden wordt (CCITT X.509/ISO 9594-8 Authentication framework).

Door in het bericht de datum en de tijd te vermelden kan worden gesignaleerd of een bericht (opzettelijk) is opgehouden.

Non-repudiation

Non-repudiation is de eigenschap die uitsluit dat de verzending van een bericht wordt ontkend. Als een bericht ontvangen is met de handtekening van een persoon A, dan vormt de handtekening het onomstotelijke bewijs dat A het bericht inderdaad getekend en verzonden heeft. Non-repudiation was bij de handmatige handtekening impliciet; er zijn niet twee personen die dezelfde handtekening gebruiken.

Uit het voorgaande blijkt dat aan een handtekening gezet door middel van een public key-algoritme deze eigenschap kan worden ontleend mits het key management goed is geïmplementeerd.

Voor symmetrische algoritmen zijn aanvullende maatregelen vereist. IBM biedt hiervoor een oplossing, het zogenaamde "control vector-principe". Met behulp van twee control vectors (één voor de zender voor het genereren van de handtekening en één voor de ontvanger voor het controleren van de handtekening) en speciale, beveiligde hardware wordt de sleutel waarmee de handtekening wordt gezet, vercijferd tot twee verschillende cryptogrammen, één voor de zender en één voor de ontvanger. Beide partijen beschikken nu over verschillende waarden ten behoeve van respectievelijk de handtekeninggeneratie en -verificatie.

Deze vorm van non-repudiation berust op de betrouwbaarheid van de hardware en de betrouwbaarheid van de systeembeheerder. De systeembeheerder is in staat de beveiliging te doorbreken door ook de andere control vector toe te voegen en het andere cryptogram te berekenen. Het is dan mogelijk de handtekening van de andere partij te berekenen. Er is dus een sterke afhankelijkheid van organisatorische maatregelen.

Non-repudiation op basis van een public key-algoritme is in dat opzicht sterker. De eigenaar van de sleutel is verantwoordelijk voor de geheimhouding van de sleutel, die uitsluitend in zijn eigen bezit is. De handtekening kan slechts worden vervalst als de sleutel uitlekt.

Tot dusver betrof het de non-repudiation door de zender; de zender is niet in staat het bericht te verloochenen. Met cryptografie kan non-repudiation van de ontvanger[12] niet worden verkregen. Non-repudiation door de ontvanger kan slechts gebaseerd zijn op aanvullende maatregelen, bijvoorbeeld de ontvangstbevestiging. De ontvangstbevestiging kan zelf ook weer worden beveiligd met een elektronische handtekening.

Vertrouwelijkheid

Door middel van een handtekening wordt geen vertrouwelijkheid van data verkregen. Als de data toch vertrouwelijk behandeld dient te worden, bijvoorbeeld koers- of concurrentiegevoelige informatie, dan is versluieren[13] mogelijk. De versluiering kan voor of na het plaatsen van de handtekening worden toegepast. In verband met in de literatuur beschreven aanvallen dient voor de vercijfering een andere sleutel te worden gekozen dan voor de handtekeninggeneratie.

Non-repudiation door de ontvanger kan slechts gebaseerd zijn op aanvullende maatregelen, bijvoorbeeld de ontvangstbevestiging.

AANSLUITING OP DE ORGANISATIE

Bij de ontwikkeling van de standaard is rekening gehouden met implementaties van organisatorische structuren. Bijvoorbeeld is rekening gehouden met meervoudige procuratie. Indien twee procureurs beiden hun fiat moeten verlenen alvorens een transactie doorgang kan vinden, dan dienen beiden de transactie te voorzien van een elektronische handtekening op basis van een persoonlijke sleutel. Er moet dan een keuze worden gemaakt tussen "nesting" of "concatenatie" van de handtekeningen.

Nesting houdt in dat de tweede handtekening geplaatst wordt over de data plus de eerste handtekening. Nesting houdt daardoor kans op problemen in, daar de verificatie van de handtekening in dezelfde volgorde dient plaats te vinden als de generatie van de handtekeningen. Er dient dus een eenduidige volgorde te worden bepaald, waarvan nooit kan worden afgeweken.

Bij concatenatie van de handtekeningen treedt dit probleem niet op. De tweede handtekening wordt net als de eerste handtekening berekend over uitsluitend de data zelf. De volgorde van verificatie is dus onafhankelijk van de volgorde van generatie. Om deze reden is door de NVB gekozen voor concatenatie.

KARAKTERSETTRANSLATIE EN KARAKTERREPRESENTATIE

Als over een hoeveelheid data een controlegetal wordt berekend, bijvoorbeeld een hash of een elektronische handtekening, dan dient de data eerst te worden vertaald naar een vorm waarmee kan worden gerekend. Als over het woord "computer" een hash wordt berekend, kan dit geschieden door voor elk karakter de bijbehorende ASCII-waarde te nemen en op basis van deze getallen het hash-algo-

12 Non-repudiation van ontvangst: met deze beveiligingsfunctie verkrijgt de verzender van een bericht het onweerlegbare bewijs dat het bericht door de ontvanger is ontvangen. Hiermee is het beschermd tegen elke poging van de ontvanger om vervolgens te ontkennen dat het bericht is ontvangen en dat de verantwoordelijkheid is aanvaard.

13 Versluiering/vercijfering: de cryptografische transformatie van data (ISO DIS 7498-2 Security architecture).

Mw. drs. M.C. van Lith Is in 1983 bij KPMG Klynveld EDP Auditors in dienst getreden en bekleedt de functie van cryptography consultant.
Zij heeft zich gespecialiseerd in de beveiligingsmethoden voor het elektronische berichtenverkeer, smart card- en magneetstripkaarttoepassingen en de onderliggende mathematische en cryptografische principes.
Zij is verantwoordelijk voor de research-activiteiten inzake de cryptografie en haar toepassingen.

ritme toe te passen. Als gekozen wordt voor een andere representatie zal dit leiden tot een andere hash-waarde. Bij het definiëren van de standaard hoort dus ook het vastleggen van de gekozen karakterrepresentatie. De NVB heeft voor de volgende hash-representatie gekozen (zie figuur 2):

Karakter	Bitpatroon
0	0000
1	0001
2	0010
3	0011
4	0100
5	0101
6	0110
7	0111
8	1000
9	1001
A	1010 1010
B	1010 1011
C	1010 1100
D	1010 1101
E	1010 1110
.	.
.	.
Z	1110 1011

Figuur 2. NVB-hash-representatie.

De NVB-hash-representatie is destijds dusdanig gedefinieerd dat cijfers slechts vier bits in beslag nemen en letters acht bits. Op deze manier kunnen financiële transacties dus in een klein formaat worden gevat. In een ASCII-representatie hebben zowel letters als cijfers een lengte van acht bits.

Als karakterrepresentatie voor de elektronische handtekening is de NVB-hash-representatie gekozen, omdat deze ook bij de NVB-hash al is toegepast en deze hash deel uitmaakt van de elektronische handtekening. Een nadeel van deze representatie is dat zij buiten Nederland niet wordt toegepast. De ASCII-representatie wordt daarentegen over de gehele wereld gebruikt.
Naast deze karakterrepresentatie wordt een translatie toegepast van het hash-resultaat naar een decimale vorm. Blokken van zestien bits worden hiertoe vertaald van de binaire naar de decimale vorm. De decimale getallen zijn eenvoudiger handmatig over te brengen tussen een calculator en een PC.

RESULTAAT: EEN VOORSTEL VOOR EEN NEDERLANDSE STANDAARD

Tijdens de ontwikkeling van de standaard is een groot aantal ideeën, problemen en bestaande implementaties geëvalueerd en besproken, uiteindelijk resulterend in een voorstel voor een Nederlandse standaard.
Hier wordt kort ingegaan op de inhoud van het voorstel voor de standaard:

- de volledige handtekening is opgebouwd uit twee lagen:
  - laag 1 is het integriteitskenmerk, de NVB-hash of indien niet mogelijk een controlegetal gebaseerd op een ander algoritme;
  - laag 2 is het authenticiteitskenmerk, de elektronische handtekening;
- de NVB-hash is gebaseerd op DES;
- voor de elektronische handtekening kan een keuze worden gemaakt uit DES en RSA[14]:
  - DES dient te worden toegepast volgens ISO 8730/8731-1, resulterend in een MAC[15] van 32 bits;
  - RSA wordt toegepast als decryptie met de secret key, waarvan de lengte minimaal 512 bits dient te bedragen;
- de toegepaste hashing-methode, het gekozen algoritme voor de elektronische handtekening en de sleutellengte worden door middel van parameters in het bericht vastgelegd;
- voor de karakterrepresentatie wordt gebruik gemaakt van de representatie voor de NVB-hash;
- voor de uitvoerrepresentatie worden blokken van zestien bits vertaald van de binaire naar de decimale vorm;
- er is een uitspraak gedaan over de minimaal in de handtekening op te nemen gegevens.

LITERATUUR

[ANSI81] ANSI X3.92, *Data Encryption Algorithm (DEA)*, 1981.

[ANSI86] ANSI X9.9, *Financial Institution Message Authentication (Wholesale)*, 1986.

[CD1191] CD 11166, *Banking - Key-management by means of Asymmetric Algorithms*, 10 juli 1991.

[FIPS88] FIPS PUB 46-1, *Data Encryption Standard*, 1988.

[ISO87] ISO 8731-1, *Banking - Approved algorithms for message authentication - Part 1: DEA-1 Algorithm*, 1 juni 1987.

[Macl92] P.G. Maclaine Pont en ir. W.H.M. Sipman, *Non-repudiation using DES control vectors and a standardized instructionset*; document number ISO/IEC JTC 1/SC 27/WG 2 N; draft version 0.2, 18 februari 1992.

[MD491] MD4 EDIFACT Security Group, *Security framework for EDIFACT*, Document 1.19 V 1.6, 14 maart 1991.

[NVB91] Nederlandse Vereniging van Banken, *NVB-hash*, mei 1991.

[NVB92] Nederlandse Vereniging van Banken, *Voorstel Standaard Authenticiteitskenmerk*, mei 1992.

[UN/E92] UN/EDIFACT Security Joint Working Group, *EDIFACT Security Implementations Guidelines*, 9 juni 1992.

14 *RSA: een asymmetrisch algoritme, genoemd naar de uitvinders Rivest, Shamir en Adleman.*

15 *MAC: Message Authentication Code. Een 32 bits-waarde die het resultaat is van een authenticatie-algoritme dat gebruik maakt van een geheime symmetrische sleutel (ISO 8730/8731-1).*

De beveiliging van elektronisch bankieren

Mw. drs. M.C. van Lith

Elektronisch bankieren, hoe veilig is dat?
In Nederland zijn inmiddels veel produkten op de markt voor elektronisch bankieren. De beveiligingsmogelijkheden van deze produkten variëren sterk, evenals het voor de gebruiker benodigde beveiligingsniveau.
In dit artikel wordt ingegaan op de beveiligingsmogelijkheden afhankelijk van het door de gebruiker toegepaste werkstation en rekening houdend met de omvang van de geldstroom.

INLEIDING

Elektronisch bankieren heeft een grote vlucht genomen. Naast de formulieren, tapes en diskettes is het nu ook mogelijk financiële transacties bij de bank aan te leveren door middel van datacommunicatie. Elektronisch bankieren biedt een aantal belangrijke voordelen. De klant kan financiële transacties initiëren en daarnaast saldo-informatie, koerslijsten en rente-overzichten ontvangen. Ook is het mogelijk een extra rekening te openen, geld te beleggen en - in de toekomst - zelfs een reis te boeken. Al deze handelingen waren in het verleden ook mogelijk, maar men moest ervoor naar de bank of de informatie werd opgestuurd. In beide gevallen levert elektronisch bankieren tijdwinst op.
Deze vorm van bankieren heeft als nadeel dat de data over een onbeschermd netwerk naar de bank wordt getransporteerd. Het is in principe mogelijk dat iemand een PTT-kast opent en de gegevens op de lijn afluistert of zelfs manipuleert. Met name de financiële transacties dienen te worden beveiligd tegen het aanbrengen van wijzigingen tijdens de datacommunicatiefase. Saldo-informatie kan vertrouwelijk zijn, er dienen dus mogelijkheden te zijn deze gegevens te beschermen tegen ongeautoriseerde kennisneming. Naast de beveiliging van de datacommunicatie dient ook aandacht te worden besteed aan de beveiliging van het werkstation.
In dit artikel wordt ingegaan op de beveiliging van elektronisch bankieren. Het beveiligingsniveau van de in Nederland beschikbare produkten voor elektronisch bankieren varieert echter sterk. Er zijn systemen die uitsluitend beveiligd zijn met een password of door middel van door de gebruiker in te toetsen controlegetallen, die per post zijn verstrekt. Daarentegen zijn er ook toepassingen die gebaseerd zijn op een hoogwaardige software-matige en hardware-matige beveiligingsoplossing en een elektronische handtekening. Dit artikel beschrijft de verschillende in Nederland gehanteerde beveiligingsvormen voor het elektronisch bankieren en geeft aan in welke richting de beveiliging zich ontwikkelt.

INDELING VAN IN NEDERLAND BESCHIKBARE PRODUKTEN

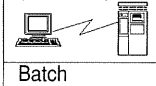
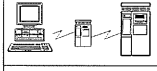
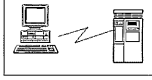
De in Nederland beschikbare produkten voor elektronisch bankieren verschillen niet alleen in beveiligingsniveau, maar ook in de wijze waarop met de bank wordt gecommuniceerd en in de gebruikte configuratie aan klantzijde. Aldus kan een indeling worden gemaakt naar communicatiewijze en naar toegepaste configuratie.
Van deze indelingen is gebruik gemaakt tijdens het ontwikkelen van het voorstel voor een Nederlandse standaard voor de elektronische handtekening door de Commissie Informatiebeveiliging van de Nederlandse Vereniging van Banken (NVB) in samenwerking met KPMG Management Consultants.

In de volgende paragrafen worden de indelingen beschreven alsmede de bijbehorende beveiligingsmogelijkheden.

COMMUNICATIEWIJZE

Ten aanzien van de gebruikte communicatiewijze is voor de produkten voor elektronisch bankieren een indeling gemaakt op applicatieniveau. Van het toegepaste communicatieprotocol op de onderliggende OSI-lagen is geabstraheerd, daar dit weinig invloed heeft op de toegepaste beveiliging. Er zijn vijf categorieën te onderscheiden, die onderling niet uitwisselbaar zijn vanwege het totaal verschillende karakter. Binnen deze categorieën kan het onderliggende communicatieprotocol variëren.
De communicatieprotocollen zijn in te delen in de volgende vijf categorieën (zie tabel 1):

Tabel 1. Communicatiewijze.

Audio response 	Door middel van een telefoontoestel wordt toegang tot de host computer verkregen. De betalingsopdracht wordt gegeven door middel van de toetsen op de telefoon. De centrale computer reageert op geluidssignalen die via de telefoonlijn binnenkomen.
Terminal (-emulatie) 	De klant verkrijgt toegang tot de host computer door middel van een terminal of een PC met een software-matige terminal-emulatie. Er wordt geen gebruik gemaakt van eventuele intelligentie van het lokale werkstation.
Batch 	Op een lokale computer worden de betalingen voorbereid. Zij worden als batch overgezonden, als hiertoe opdracht wordt gegeven. De host verwerkt de binnengekomen betalingsopdrachten periodiek.
E-mail 	De betalingsopdrachten worden naar een mailbox gestuurd. De host leest de mailbox periodiek en verwerkt de betalingsopdrachten.
Interactief 	Vanuit een intelligent werkstation worden betalingsopdrachten aan de host verstuurd door middel van een online-verbinding.

Audio response

Door middel van een telefoontoestel wordt toegang tot de host computer verkregen. De host computer meldt zich aan de gebruiker met gesproken taal. Vervolgens geeft de gebruiker de betalingsopdracht door middel van de toetsen op de telefoon. De centrale computer reageert op geluidssignalen die via de telefoonlijn binnenkomen.
Voor audio response zijn slechts weinig beveiligingsmaatregelen mogelijk. Op een standaardtelefoon is geen lokale intelligentie beschikbaar.
Beveiliging kan evenwel worden toegevoegd door gebruik te maken van een zogenaamde "calculator". De calculator is een apparaat dat controlegetallen berekent op basis van een door de host gegenereerd randomgetal of op basis van betalingsgegevens. Het berekende controlegetal (de elektronische handtekening) wordt vervolgens op het telefoontoestel ingetoetst. Elke calculator maakt voor de berekening gebruik van een unieke ingebouwde cryptografische sleutel, zodat men zich met dit apparaat kan authenticeren.

Door middel van de calculator kan een beperkt aantal betalingsgegevens worden beschermd tegen het aanbrengen van wijzigingen tijdens transport. Deze vorm van beveiliging is beter dan toepassing van een password. Het password kan tijdens communicatie worden afgetapt, daar de lijn niet wordt beschermd.

Terminal (-emulatie)

De klant verkrijgt toegang tot de host computer door middel van een terminal of een PC met een software-matige terminal-emulatie. Er wordt geen gebruik gemaakt van eventuele intelligentie van het lokale werkstation. (Indien de toepassing toch gebruik maakt van de lokale intelligentie anders dan voor het verwerken van de terminal-emulatie, dan valt de toepassing in de categorie "interactief".)

Een terminal of een terminal-emulatie kent eveneens weinig mogelijkheden tot beveiligen wegens het gebrek aan lokale intelligentie. Met behulp van de calculator kan net als bij audio response authenticatie van de zender plaatsvinden.

Er zijn grote overeenkomsten tussen audio response en de terminal-emulatie. De terminal-emulatie is gebruiksvriendelijker en veiliger, daar de door de gebruiker ingetoetste waarden op het scherm zichtbaar zijn en dus visueel kunnen worden gecontroleerd.

Batch

Op een lokale computer worden de betalingen voorbereid. Zij worden als batch overgezonden, op het moment dat hiertoe opdracht wordt gegeven. De host verwerkt de binnengekomen betalingsopdrachten periodiek.
Als de batch gereed is voor verwerking, berekent de klant over de gehele verzameling betalingsopdrachten een NVB-hash[1] gevolgd door een elektro-

nische handtekening over het hash-resultaat. De batch en de handtekening worden vervolgens door middel van datacommunicatie verzonden naar de computer van de bank.
Aandacht dient te worden besteed aan het bewaren van de integriteit van de betalingsopdrachten tijdens de opbouw van de batch.

E-mail

De betalingsopdrachten worden naar een mailbox gestuurd. De host leest de mailbox periodiek en verwerkt de betalingsopdrachten.
Een betalingsopdracht wordt beveiligd door middel van de NVB-hash en de elektronische handtekening. Er zijn overeenkomsten met de batch-verwerking. Voor zowel batch- als E-mail-verwerking wordt een communicatiewijze gehanteerd met een store and forward-karakter, dit in tegenstelling tot de andere drie categorieën.

De verschillen tussen batch-verwerking en E-mail liggen voornamelijk op het vlak van de aanvullende beveiligingsmaatregelen. Bij de batch-verwerking dient aandacht te worden besteed aan het bewaren van de integriteit tijdens het opbouwen van de batch. Bij E-mail wordt de aandacht gericht op de beveiliging tijdens bewaring in de mailbox.

Interactief

Vanuit een intelligent werkstation worden betalingsopdrachten aan de host verstuurd door middel van een online-verbinding. Zowel op de host computer als op het werkstation draaien applicaties die met elkaar communiceren. De applicatie op het werkstation kan ook bestaan uit een terminal-emulatie uitgebreid met een hot key-functie, waarbij door middel van een hot key uit de terminal-emulatie kan worden gesprongen. De transactie-aanvragen worden evenals bij audio response en terminal(-emulatie) real time verwerkt.

De gehele communicatie of een deel ervan wordt beveiligd met een NVB-hash en een elektronische handtekening.

TOEGEPASTE CONFIGURATIES

De Nederlandse produkten voor elektronisch bankieren kunnen qua toegepaste klant-configuratie worden ingedeeld in vijf klassen. De klassen hebben een verschillend fysiek beveiligingsniveau. Tevens bieden de klassen verschillende mogelijkheden voor de implementatie en ondersteuning van interne-controlemaatregelen.
In deze paragraaf wordt eerst een beschrijving gegeven van toegepaste beveiligingscomponenten en vervolgens wordt ingegaan op de vijf klassen en hun beveiligingsniveau.

Beveiligingscomponenten

De volgende beveiligingscomponenten worden in de beschreven configuraties toegepast:

Calculator
De calculator is een klein apparaat met een display en cijfertoetsen. De gebruiker krijgt toegang tot de calculator door het juiste PIN in te toetsen.
De calculator kan op twee manieren worden gebruikt:

1. genereren van een elektronische handtekening over de betalingsgegevens.
De calculator berekent de elektronische handtekening op basis van betalingsgegevens, een cryptografisch algoritme en een geheime sleutel.

2. toegangsbeveiliging.
De calculator berekent een controlegetal op basis van een door de host computer berekende random waarde, een cryptografisch algoritme en een geheime sleutel (challenged response).

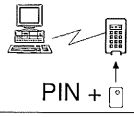
Er is geen verbinding tussen de calculator en het werkstation. De gegevens dienen dus handmatig te worden overgebracht tussen het werkstation en de calculator.

De smart card-lezer is in tegenstelling tot de calculator online met het werkstation verbonden en is daarom gebruiksvriendelijker.

Smart card-lezer
De smart card-lezer is in tegenstelling tot de calculator online met het werkstation verbonden en is daarom gebruiksvriendelijker. De gebruiker krijgt toegang tot het werkstation door middel van de smart card en het bijbehorende PIN.
De smart card-lezer heeft over het algemeen een hoger beveiligingsniveau dan de calculator, daar de beveiliging is gebaseerd op smart card-technology. Soms worden calculators echter met een zelfde chip uitgerust en bieden dan dus hetzelfde beveiligingsniveau. De smart card-lezer is duurder dan de offline-calculator.

Security board
Een security board is een kaart die in de PC wordt geplaatst. De kaart is voorzien van een hardwarematige beveiliging, die voorkomt dat cryptografische sleutels worden uitgelezen. Het security board heeft een snellere processor dan een smart card, zodat het security board de configuratie geschikt maakt voor grote aantallen transacties.

1 *Voor een toelichting op de NVB-hash wordt verwezen naar het artikel 'Een Nederlandse standaard voor de elektronische handtekening', opgenomen in deze Compact.*

Software only 	De beveiligingsmaatregelen zijn uitsluitend software-matig geïmplementeerd. Er is geen fysieke beveiliging.	batch, E-mail, interactief
Calculator offline of 	De elektronische handtekening wordt in de calculator berekend en wordt handmatig naar de telefoon of terminal overgebracht.	audio response, terminal(-emulatie)
PC + calculator offline 	De in de PC berekende hash wordt handmatig overgebracht naar de calculator, waar de handtekening wordt berekend. De handtekening wordt vervolgens handmatig naar de PC overgebracht.	batch, E-mail, interactief
PC + smart card online  PIN +	De in de PC berekende hash wordt automatisch overgebracht naar de calculator, waar de handtekening wordt berekend. De handtekening wordt vervolgens automatisch teruggetransporteerd.	batch, E-mail, interactief
PC + security board + smart card online  PIN +	Naast de PC en smart card-lezer wordt gebruik gemaakt van een security board, die in de PC is geplaatst. De berekening van de hash en die van de elektronische handtekening vinden beide plaats binnen het security board.	batch, E-mail, interactief

Tabel 2. Configuraties.

De configuraties zijn in te delen in de vijf in bovenstaande tabel 2 genoemde klassen.

Software only

De beveiligingsmaatregelen zijn uitsluitend software-matig geïmplementeerd. Er wordt geen gebruik gemaakt van aanvullende beveiligingsmaatregelen zoals een calculator, een smart card-lezer of een security board.
Cryptografische sleutels ten behoeve van de berekening van de elektronische handtekening kunnen in deze configuratie slechts matig worden beschermd. De bescherming van de sleutels berust op het "verstoppen" van de sleutels in de software of de databestanden of het vercijferen van de sleutelbestanden op basis van een in te voeren password. Een alternatieve beveiligingsoplossing wordt geboden door de software op een floppy in een afgesloten ruimte te bewaren.

Deze configuratie wordt toegepast voor relatief kleine bedragen en kleine aantallen transacties. De host computer dient geen hoge bedragen te accepteren. Het risico blijft onder deze omstandigheden beperkt. Als een bedrijf een relatief klein aantal transacties van uitsluitend lage bedragen uitvoert, is het aanschaffen van aanvullende hardware-matige beveiliging niet rendabel.

Calculator offline

Door toepassing van een calculator biedt deze configuratie een hoger beveiligingsniveau dan "software only". De door de calculator berekende elektronische handtekening verschijnt op het display van de calculator en wordt vervolgens handmatig ingetoetst op de terminal of de telefoon van de klant. Afgezien van de calculator is er geen lokale intelligentie beschikbaar.

Wegens dit gebrek aan lokale intelligentie kan op het werkstation geen hash worden berekend. Op de calculator worden het bedrag, het rekeningnummer van de begunstigde, de procuratiegegevens en eventueel het rekeningnummer van de betalende partij ingevoerd. De ingevoerde gegevens worden geconcateneerd en vervolgens wordt hierover een handtekening berekend.

De configuratie is geschikt voor lage tot middelgrote bedragen. Wegens de gebruiksonvriendelijkheid, veroorzaakt door de veelvuldige handmatige invoer, is de configuratie niet geëigend voor grote aantallen transacties.

De calculator wordt te duur als naast de elektronische handtekening tevens de NVB-hash-functie geïmplementeerd dient te worden. Doordat de calculator wordt gebruikt in een omgeving waarin slechts kleine aantallen transacties van lage bedragen worden gegenereerd, zijn hoge kosten voor beveiligingsmaatregelen niet gerechtvaardigd.

PC plus calculator offline

Door de aanwezigheid van lokale intelligentie in de PC is het mogelijk een hash-berekening over de betalingsopdracht uit te voeren en de calculator te gebruiken voor het genereren van de elektronische handtekening. Het op de PC berekende hash-resultaat dient hiertoe te worden ingebracht in de calculator. Na berekening van de elektronische handtekening in de calculator dient vervolgens de handtekening weer op de PC te worden ingevoerd.

De configuratie is net als de configuratie zonder PC geschikt voor kleine tot middelgrote bedragen en is wegens de veelvuldige handmatige invoer niet geschikt voor grote aantallen transacties.

PC plus smart card online

Naast de PC wordt gebruik gemaakt van een met de PC verbonden smart card-lezer. De berekeningen vinden plaats op dezelfde wijze als bij "PC plus calculator offline". Het voordeel van deze configuratie boven de "PC plus calculator offline" is dat de berekende controlegetallen niet handmatig overgenomen hoeven te worden. De configuratie is daarom geschikt voor grote aantallen transacties.
De smart card biedt over het algemeen een hoger beveiligingsniveau dan de calculator. De configuratie is derhalve geschikt voor middelgrote bedragen.

PC plus security board plus smart card online

Naast de PC en smart card-lezer wordt gebruik gemaakt van een security board, die in de PC is ge-

plaatst. De berekening van de hash en die van de elektronische handtekening vinden beide plaats binnen het security board.
Deze configuratie is net als de configuratie zonder security board geschikt voor grote aantallen transacties, daar menselijke handelingen slechts beperkt nodig zijn. Bovendien biedt het security board een hogere verwerkingssnelheid.

De toevoeging van het security board maakt de configuratie geschikt voor hoge bedragen, bijvoorbeeld overboekingen van bank naar bank.

KEY MANAGEMENT

Het gebruik maken van cryptografische beveiliging impliceert dat maatregelen van key management moeten worden getroffen. Vooral multibanktoepassingen hebben consequenties voor het (initiële) key management.

Multibank

Een multibank-toepassing is een toepassing waarbij het mogelijk is financiële transacties uit te wisselen met verschillende banken. Binnen de applicatie moeten er mogelijkheden zijn om de sleutels voor de beveiliging van de communicatie met de verschillende banken in te voeren.

Het initiële key management is voor multibanktoepassingen complexer dan voor de normale single bank-toepassingen. Het inbrengen van de sleutels van de verschillende banken dient op een veilige wijze te geschieden. De ene bank mag de sleutel van de andere bank niet in klare vorm beschikbaar krijgen.

Als gebruik wordt gemaakt van een symmetrisch algoritme voor het inbrengen van de werksleutels, dan leidt dit tot meer organisatorische problemen dan bij een asymmetrisch algoritme, daar voor alle deelnemende banken een symmetrische transportsleutel in klare vorm moet worden ingebracht. De bank zal de transportsleutel niet bekend willen maken en deze tijdrovende handeling zelf uitvoeren. De werksleutels kunnen vervolgens vercijferd onder deze transportsleutel worden geladen. Het is belangrijk dat de sleutels van de verschillende banken niet worden verwisseld.

Als daarentegen van een public key-algoritme gebruik wordt gemaakt, kan het initiële key management worden vereenvoudigd door in het werkstation (binnen de beveiligde omgeving) een public key-paar te laten genereren. De public key wordt aan de bank bekend gemaakt en vervolgens kan de bank de werksleutel onder de public key vercijferen door middel van een asymmetrisch algoritme. Het cryptogram kan door de eigenaar van het werkstation worden ingevoerd, omdat het cryptogram uitsluitend door de eigenaar van de secret key is te ontcijferen. Bij deze methode is tussenkomst van een medewerker van de bank niet nodig. Er dienen echter wel aanvullende maatregelen te worden getroffen ten aanzien van de integriteit van de door het werkstation gegenereerde public key. Dit probleem kan worden opgelost met een handmatig getekend formulier dat per post wordt verzonden.

Een te vertrouwen derde partij

Het instellen van een instantie als "trusted third party" kan praktische voordelen hebben ten aanzien van het key management.

Als aan een netwerk een knooppunt wordt toegevoegd, dan zal het nieuwe knooppunt met alle knooppunten waarmee hij wil communiceren contact moeten zoeken, zich authenticeren, eventueel specifieke afspraken maken en ten slotte sleutels uitwisselen. Het uitwisselen van de initiële sleutel is een procedure die extra beveiligingsmaatregelen behoeft, daar deze sleutel niet kan worden vercijferd. Meestal komt het erop neer dat een medewerker van de ene partij de sleutel aan de andere partij brengt, een tijdrovende en dure procedure.

Het instellen van een instantie als "trusted third party" kan praktische voordelen hebben ten aanzien van het key management.

Een trusted third party, die functioneert als key management-centrum, maakt het toevoegen van een partij eenvoudiger. De initiële sleutel hoeft slechts te worden uitgewisseld tussen de nieuwe partij en de trusted third party. Alle overige sleutels kunnen door middel van datacommunicatie en vercijfering worden uitgewisseld, omdat voor de overige gekoppelde partijen de initiële sleuteluitwisseling met de trusted third party reeds heeft plaatsgevonden.
Als gebruik wordt gemaakt van een public key-algoritme maakt de aanwezigheid van een trusted third party het key management eveneens eenvoudiger. De nieuwe partij deponeert de door hem gegenereerde public key bij de trusted third party. De trusted third party verspreidt deze sleutel voorzien van een certificaat[2] aan de overige knooppunten door middel van datacommunicatie. Elke partij wordt bij initialisatie voorzien van de public key van de trusted third party, zodat het certificaat kan worden gecontroleerd.

Afhankelijk van de toepassing zijn kandidaten voor de rol van trusted third party: de BGC, BeaNet, PTT- Telecom en moedermaatschappijen van grote concerns. In Nederland worden "handmatige" handtekeningen gedeponeerd bij de Kamer van Koophandel. Het is niet ondenkbaar dat deze functie in de toekomst wordt uitgebreid tot elektronische handtekeningen.

2 *De publieke sleutel van een gebruiker die samen met enige andere informatie onvervalsbaar wordt gemaakt door een vercijfering met een geheime sleutel van de certificerende instantie die het certificaat heeft uitgegeven (CCITT X.509/ISO 9594-8 Authentication framework).*

Mw. drs. M.C. van Lith
Is in 1983 bij KPMG Klynveld EDP Auditors in dienst getreden en bekleedt de functie van cryptography consultant.
Zij heeft zich gespecialiseerd in de beveiligingsmethoden voor het elektronische berichtenverkeer, smart card- en magneetstripkaarttoepassingen en de onderliggende mathematische en cryptografische principes.
Zij is verantwoordelijk voor de research-activiteiten inzake de cryptografie en haar toepassingen.

BLIK OP DE TOEKOMST

Het voorspellen van de toekomst op een zich snel ontwikkelend terrein is moeilijk; toch wil ik ter afsluiting van dit artikel hierover iets zeggen. Gezien de dalende prijzen van elektronica en de ontwikkelingen op het terrein van de telefoon kan het volgende worden verwacht:

- De offline calculator zal op den duur verdwijnen omdat de kosten van de gebruiksvriendelijker online-apparatuur omlaag gaan.

- De software only-configuratie zal op den duur minder worden toegepast doordat aanvullende hardware goedkoper wordt.

- Audio response zal zich ontwikkelen in de richting van de "smart phone", een telefoontoestel met interne intelligentie, zodat offline-apparatuur niet nodig is. Enkele leveranciers hebben al een dergelijk toestel beschikbaar. Deze toestellen zijn beveiligd door middel van een smart card.

- De configuratie van de toekomst wordt een PC met smart card en eventueel een security board. De smart phone met de ingebouwde computer staat niet zover meer van de PC-toepassing af.

LITERATUUR

[Guli91] Drs. H.J. Guliën, *Electronic banking in kort bestek*, brochure KPMG Klynveld Management Consultants, september 1991.

[NVB92] Nederlandse Vereniging van Banken, *Voorstel Standaard Authenticiteitskenmerk*, mei 1992.

Secure Cash Management

a case study

H. Roos RA and H. Veenman MBT

Beveiligingsstandaarden voor electronic banking, cash management en EDI vertonen nog tekortkomingen. Toch wilde Cargill overgaan tot invoering van deze nieuwe technologie.
Roos en Veenman waren als beveiligingsdeskundigen bij dit project betrokken. Vanuit deze ervaring behandelen zij de valkuilen en gekozen oplossingen om te komen tot een voldoende beveiligde omgeving.

SUMMARY

During the design of a new Cash Management System (CMS), Cargill BV in Amsterdam identified a number of security problems. Key of the solution was the application of cryptographic technology. However, this caused problems with the interfacing of the system with the electronic banking software which was in use.
The solution required the clear separation of the responsibility for the processing of payment orders on the company's side and on the bank's side. The interface between both had to be a common file or message format. It was decided to use the UN/EDIFACT standard for payment orders. In view of a lack of standardization of the security for the payment order messages it was decided to use the most recent proposal of the UN/EDIFACT Security Working Group.

This article gives an impression of the development of the CMS with a focus on Electronic Data Interchange and related security issues.

Due to the fact that chipcard technology and cryptographic techniques are used in a practical business application, where multiple parties were committed to the results, this project is supported by a grant from the Dutch government as part of the "Telematica gidsprojecten 1992" programme.

INTRODUCTION

Cargill is a U.S.-based company, trading, processing and transporting all kinds agricultural goods. Its global headquarters are in Minneapolis. Apart from offices and plants in the North America Cargill is also located in the Latin America, the Pacific Rim and Europe.
The Benelux headquarters are based in Amsterdam.
The turnover of the Dutch company, Cargill BV, was more than 5 billion Dutch guilders in 1991.
Data processing is based on IBM AS/400 midrange computers. Terminals (5250) and PS/2 workstations are connected to the AS/400 systems via twinax and token ring networks, respectively.

The Cash Management System

The basic function of the Cash Management System is to allow the preparation of payment orders, their forwarding to the banks for settlement, while providing enviroment for this.

Payment Order Preparation
One of the objectives of the Cash Management System[1] is to perform the payment of funds to trading partners, which may be banks with respect to foreign exchange contracts or corporations for trade contracts.
This process is time-critical because of the demand in commodity trading for correct and timely payment. The exact timing of payment is influenced by the amounts involved, the different currencies and interest rates, the volatility of the foreign exchange market and the different clearing processes of the central banks.

In the existing CMS payment is performed at plant level. Invoices are first checked for correctness with respect to purchase agreement and delivered quantities and qualities. After these controls the invoices are paid by the local cash manager.

Use of electronic banking applications
Every day the local cash manager selects the payment orders to be settled, the bank to which they should be forwarded and the accounts to be debited. Payment is done by means of terminals on which electronic banking (EB) software, provided by the banks, runs. The payment orders are sent from the terminal to the bank using a direct modem connection. Use of the EB-software is only possible by authorised staff. Control is performed by means of passwords.

Inherent security risks
The objective of designing a new Cash Management System was to centralise cash management and settlement. This implied the necessity of local impact of payment orders (at plant level) and central processing. Although all sites have processing capabilities and terminal facilities, communications between the plants and the central office use unsecure communication channels. Therefore, in order to prevent unauthorized modifications of payment orders remaining undetected, a second check at corporate level with all related documents would be required.
This would imply the need to physically send those documents to the central office. It is clear that the time required to do this would neutralise the speed gained by using data communication.
Another weakness was the possibility of interception of logon data on networks and PC's, including passwords. This would make the system vulnerable to modifications and even insertion of payment orders at points where detection is very unlikely.
This could even be performed by a fully authorized person who has normal access to the EB-PC's, due to the fact that the EB-applications allow payment order information to be added or modified.

The security features of the AS/400 are used to control access to the data and applications on those systems. If properly designed the risk of unauthorized access to data and programs can be restricted to a small number of staff, possibly only to the security officer. However, this requires the application of level 40 security. The problem with this is the likelihood that special programs which explore the AS/400 machine interface and are not supplied by IBM will no longer run. This was considered an important reason to investigate other, more secure solutions.

The project

Early in 1991 Cargill asked KPMG to give their opinion on the possibilities for solving the security problems described above, which are related to the design of their new Cash Management System. Due to the integration of parts of the approval and treasury functions in one information system which is intended to run on a network of AS/400 computers, security exposures arose relating to the integrity and authentication of payment orders.

It was soon clear that a combination of technological and procedural measures was a possible means of solving the problem. The application of standard cryptographic technology was considered a key element in the solution.
It was decided to explicitly include the security aspect in the project for the development of the new CMS. After initial global design and discussions with the Cargill's banks and several suppliers of cryptographic technology it became clear that IBM cryptographic technology was the most obvious choice.

Electronic Data Interchange (EDI) was introduced during the first phase of detailed design. After having considered the possibility of maintaining the existing electronic banking systems (EB) for the exchange of financial messages between Cargill and banks A and B, the problem of securely interfacing the CMS with those EB-systems appeared too complex to be practically manageable.
It was decided to consider the use of common EDI formats instead. This has the advantage of a clear

1 *Important: For reasons of confidentiality some aspects of the Cash Management System are only discussed on a conceptual level and details are intentionally omitted.*

segregation of responsibility between the corporation and the related banks.
As a consequence of this decision the project was extended with an EDI component, which had to be strongly intertwined with the designed security solutions.
The UN/EDIFACT formats for payment orders were selected as most sensible candidates. The selected format will be explored later in this article.
However, the security component of those formats is still under discussion. As a basis for the implementation, a proposal of the MD4 EDIFACT Security Group was adopted [MD491]. The security framework proposed by MD4 is considered to be sufficiently flexible for incorporation of security information into the interchanges between company and bank.
During implementation and testing however, a number of deficiencies in this framework have been identified, for which arbitrary, practical solutions had to be adopted.
Another issue is the limitation of the MD4 proposal concerning company to bank interchanges. During design and testing on the basis of actual data it was considered illogical and uneconomical to be forced to convert formats according to the different bank-to-bank payment networks to be used (S.W.I.F.T., CHAPS, CHIPS, FEDWIRE, etc.).
As of 31 October, 1992 the new Cash Management System went live, with the security related software and hardware components. After a local trial period of several months the CMS is intended to be implemented in other central offices of the Cargill enterprise.

The correct and far-reaching application of information technology enables Cargill to optimize its Cash Management business process from Approval to Treasury and beyond.

SELECTION OF THE CORRECT SOLUTION

The selection of the correct solution was dependant on the interface facilities with EB sytems and the level of security provided

Interfacing issues

As stated earlier, the preliminary design assumed the continued use of the EB systems provided by the banks.
However, the timely detection of any unauthorized addition or modification of payment orders required the integration of final check and transmission of payment orders in one secure domain on the EB PC.
This was not possible without modification to the EB applications themselves.
The necessary disclosure of the source code and the need for future changes of the interface between the CMS and the EB systems would result in a grey area which would make it very difficult to identify a responsible party in case of failures. Moreover, this approach would require redesign and reprogramming of the interface with any new clearing bank. This would be the case when the CMS would, as anticipated, be implemented at Cargill locations in other countries. So this was not an acceptable solution.

The correct and far-reaching application of information technology enables Cargill to optimize its Cash Management business process from Approval to Treasury and beyond.

A clear segregation of responsibilities between company and bank would be provided by a common interface format and agreement about the security measures for authentication of the sender and verification of the actual message contents.
On this basis it was decided to adopt a common interchange format, with each party being responsible for the correct implementation of the sending and receiving software.

Security related issues

In the preliminary design of the new CMS it was anticipated that, in addition to the coverage of the above mentioned weaknesses, the flow of paper based invoice control documentation should stop at plant level, that modifications by unauthorized staff should be detectable in good time and that any deficiencies in AS/400 security should not jeopardize the CMS security.

Key to the security solution is the use of cryptographic technology. Use of the standard AS/400 cryptographic facility was discarded because this does not provide for secure storage of cryptographic keys. It is in fact a software solution which can be made considerably secure if applied in conjunction with AS/400 level 40 security, which was not installed.
Moreover, this would not fully solve the vulnerability for logon password interception and for the security officer. As a result, a basic decision was made to separate the CMS security from the AS/400 security.
The cryptographic facility is based on the Transactions Security System from IBM. (See [Vrie92].)
The payment orders which are created at plant level are secured with a Message Authentication Code (MAC) at the moment of final approval and sent up to the central AS/400.
Before the payment order is transmitted to the bank, this MAC is verified and after modification (into the interchange format) and addition of some fraud-insensitive information a second MAC is calculated which is used by the bank to check the integrity and the authenticity of the payment order.
The final approval of payment is done by different staff then the staff performing the actual transmittal of payments to the bank. This segregation of

duties is supported by the technology used.
The control vector concept [Vrie92] is applied in combination with the DES encryption algorithm to prevent generation of a MAC by the verifying party.
Logon to the PC's on which payment order approval (and MAC-ing) is performed, is secured with a personal security card (chip card) and an electronic signature pen. The same security applies to the corporate treasury PC for MAC verification and second MAC calculation. The transmission of the payment orders is performed by the standard AS/400 communications facilities.

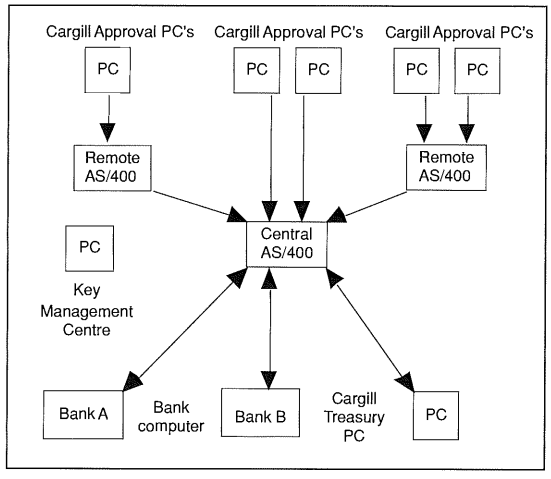


Figure 1. Secure CMS Configuration.

Figure 1 gives an impression of the configuration of the Secure CMS as implemented at Cargill.
Duplications of messages and message replay prevention and detection required additional measures. This problem was solved by means of a table containing the id of each transmitted payment order including a date and time stamp. On transmission to the bank, acceptance by the bank or rejection, a status code in the table is updated. Each payment order is checked against this table with status codes, to prevent double payments.
The integrity of the table is secured with a MAC.

Key management

The security of the Cash Management System is based on the secrecy of the cryptographic keys involved. Even in a "simple" application like the CMS a large number of different types of cryptographic keys are required. The most important key types are:
- Workstation Security Keys;
- Key Distribution Security Keys;
- Internal Message Security Keys;
- External Message Security Keys;
- File Security Keys.

Of extreme importance therefore is a strict organisation of Key Management. Two people are held responsible for operational key management. Key management takes place in and around a secure Key Management Centre. The Key Management Centre (KMC) consists of a PS/2 including TSS Cryptographic Adapter, Personal Security Card reader, Signature Verification Kit and EPROM chip for boot protection.

The Key Management Centre (KMC) is, furthermore, physically shielded against unauthorized opening of the PC housing and against unauthorized use of the diskette drive. Access to the KMC is limited to authorized personnel by placing the configuration in a secure room.

In-house development

The main objective of explicitely integrating security in the CMS development project was to strive for the practical realisation of the required level of end-to-end security. On the basis of this objective it was decided to have KPMG develop the security software modules, including MAC generation and verification and internal-to-EDIFACT conversion, instead of building a system out of multiple "off-the-shelve" software products. Practical reasons were:
- confidentiality of the exact design and operation of the secure parts of CMS;
- lack of availability of EDIFACT conversion tools that support a security framework;
- expected overhead due to the introduction of multiple products from multiple independent vendors.

THE USE OF STANDARDS

The objective of the CMS project was and is to enhance the efficiency and effectiveness of the cash management operation, and to optimize competitiveness. Not only in the Benelux, but worldwide. For that purpose all CMS interfaces with the outside world had to be based on accepted standards, to allow compatibility with other Cash Management Systems and with other banks. For this project a selection has been made out of the available commonly accepted standards or draft standards. Three of those are discussed in the following subparagraphs: ANSI X9.9 (equivalent to ISO 8730/31), EDIFACT and the EDIFACT Security Framework.

ANSI X9.9

End-to-end authentication of the payment order message is established by calculating a Message Authentication Code over the critical fields in the payment order. The algorithm selected for this project for calculation of the MAC is described in ANSI standard X9.9 (1986 edition). A block diagram of the algorithm is shown in figures 2a and 2b.
As shown the algorithm is based on a maximum string input of 64 Kbytes long. Figure 2b shows how the algorithm can be repeated in the event of longer strings.
The encryption algorithm (E) used, is the Data

Encryption Standard (DES). The key for the MAC calculation (K) is generated internally by means of the KMC if it concerns the internal MAC and externally by the bank if it concerns the MAC that is used by the banks to check the integrity and authenticity of the payment orders. In both cases a secure procedure is established to periodically load keys in the corporate systems.

The TSS hardware supports the use of the ANSI X9.9 standard; an extensive set of programming interface calls are available for the development of specific applications.

EDIFACT

The starting positions of all parties involved was to continue using the existing formats used in their own systems and introduce an intermediate exchange format.
This would require conversion from an internal CMS-format to an exchange format by Cargill and conversion from exchange format to internal Bank format by Banks A and B. After detailed consideration of the proposed interchange format all three parties involved have identified the modification of their internal formats as most appropriate.
Figure 3 shows the directory of available message types provided by the UN/EDIFACT. The structure of each type is similar. Messages consist of standard data elements, grouped in segments.

Figure 3. United Nations Standard Message Types Directory (EDMD).

CREADV	Credit advice
CREEXT	Extended credit advice
CUSCAR	Customs cargo report
CUSDEC	Customs declaration
CUSREP	Customs conveyance report
CUSRES	Customs response
DEBADV	Debit advice
IFTMAN	Arrival notice
IFTMBC	Booking confirmation
IFTMBF	Firm booking
IFTMBP	Provisional booking
IFTMCS	Instruction contract status
IFTMIN	Instruction message
INVOIC	Invoice message
ORDERS	Purchase order message
PAYEXT	Extended payment order
PAYORD	Payment order
REMADV	Remittance advice

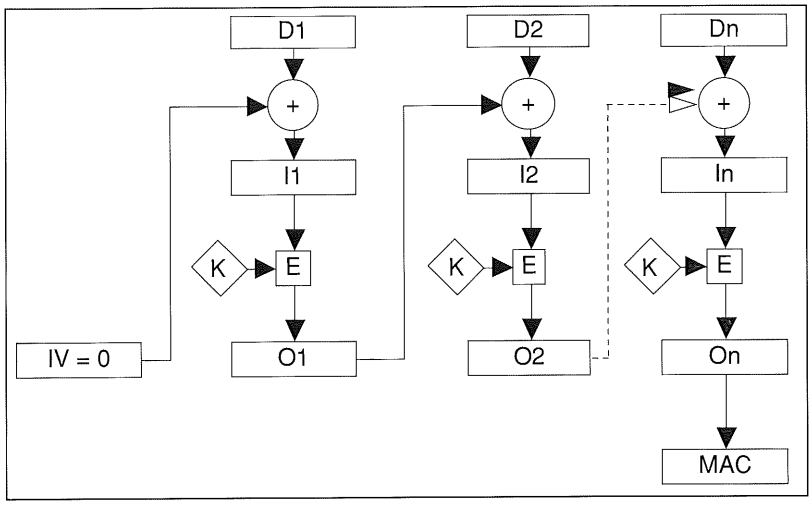


Figure 2a. MAC calculation.

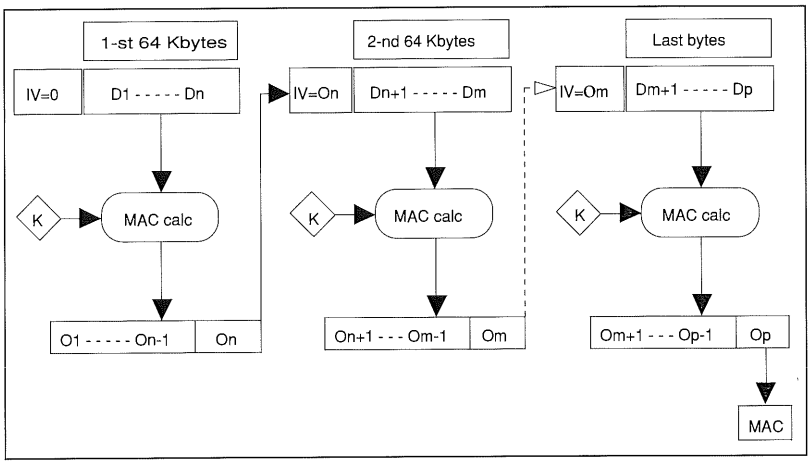


Figure 2b. MAC calculation in case of more than 64 Kbytes of data.

Multiple messages are combined in functional groups, which in their turn combine into an interchange.
Each element, segment, group, etc. is identified with a header, sometimes ended by a trailer. Figure 4 shows the generic structure of an EDIFACT interchange. For CMS the message type PAYORD was chosen.

Although PAYORD was the most obvious and best-fitting message type to select and although substantial detailed documentation is available on this matter, considerable effort was needed to define and agree upon the exact (sometimes conditional) contents of each simple data element. The message type specification of PAYORD is shown in figure 5.
Explicit attention had to be given to the inclusion of the pertinent information. This appeared to require a higher level of discipline from the trading

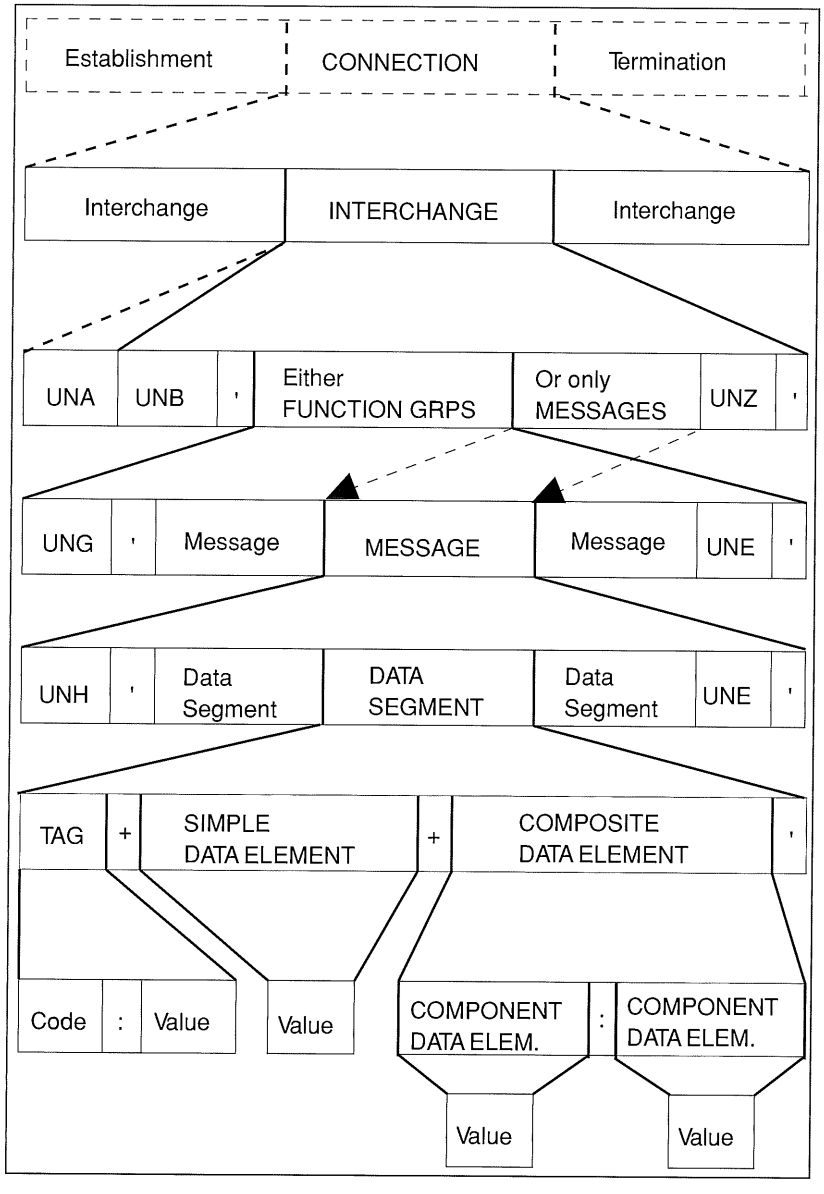


Figure 4. Hierarchical structure of an interchange.

TAG	NAME	S	REPT	S	REPT
UNH	Message header	M	1		
BGM	Beginning of message	M	1		
BUS	Business function	C	1		
	Segment Group 1			C	6
NAD	Name and address	M	1		
CTA	Contact information	C	1		
COM	Communication contacts	C	1		
	Segment Group 2			C	4
FII	Financial Institution Information	M	1		
CTA	Contact information	C	1		
COM	Communication contacts	C	1		
DTM	Date / Time / Period	M	2		
	Segment Group 3			C	4
INP	Parties of instruction	M	1		
FTX	Free text	C	1		
DTM	Date / Time / Period	C	2		
PAI	Payment instructions	C	1		
FCA	Financial charges allocation	C	1		
	Segment Group 4			M	1
MOA	Monetary amount	M	1		
CUX	Currencies	C	1		
RFF	Reference	C	1		
FTX	Free text	C	1		
DOC	Document/message details	C	10		
	Segment Group 5			C	2
NAD	Name and address	M	1		
FTX	Free text	M	6		
AUT	Authentication result	C	1		
UNT	Message trailer	M	1		

Figure 5. Message type specification PAYORD.

partners, because this information should be provided to a large extent on the invoice which in our case is the starting point for the construction of the payment order.
Another unsolved problem is the information which is needed for central bank reporting. This may differ per nation and even between different banks within one nation. It is contained in the UN/EDIFACT format as unstructured text. This requires consequently additional message repair actions.

EDIFACT Security Framework

The standards for the generation and verification of DES-based MAC's are clear and well-defined. The MAC's, however, should be included in the exchange format in the right positions.

This latter issue could not be solved satisfactorily by the use of an actual standard. The MD4 proposal of March 1991 [MD491] was selected as a basis. The scope of this standard is company to bank, taking into account company to company information exchange needs.

The security framework is designed as a shell around the data elements, functional groups and interchange.
However, the MD4 security framework defines the data stream to be input into the MAC calculation starting with the first character of the interchange header up to the character immediately preceding the security trailer segment. This leaves the message trailer which contains sequence information outside of the scope of the MAC. A risk results that messages are added or deleted at the trailing end of the interchange. This can be overcome by mak-

ing it possible to identify specific segments to be part of the data stream for MAC generation or by MAC-ing at interchange level.

Although the MD4 proposed security framework is sufficiently flexible to permit security segments at different interchange levels (message, functional group, interchange), the June 1992 proposal of the UN/EDIFACT Security Joint Working Group [UN/E92] seems to restrict security to message level. Work is continuing to improve on this by the adoption of a new message type (AUTHEN) which permits authentication of multiple messages, but a concrete standard on security of EDI messages is not expected before September 1993.

CONCLUSIONS

The full benefits of financial EDI requires integration of the corporate process and the bank process. The key to this integration is the reconciliation of the corporate to bank exchange format with the various bank-to-bank formats. Figure 6 depicts the schematics of Secure Electronic Banking as implemented in the project described in this article.
Standardization of the security of financial EDI exchanges is urgent.

A particular problem not dealt with in this article is the policy of western governments regarding the licensing of DES and RSA (crypto technology in general). Although the Cargill solution does not provide for message confidentiality - the MAC is calculated using DES, but the message itself is not encrypted! -, the MD4 framework explicitly mentions this as one of the basic security functions for an EDI system. This is actually frustrated by the denial of DES licenses for the purpose of encryption of information. Even to well-known global enterprises which require these facilities to maintain their competitiveness [IEEE92]. The controversy between industry and governments must be solved as soon as possible.
The forthcoming OECD guidelines on the security of information systems may possibly expedite such a solution [OECD92].

The audit aspects of Cargill's new Cash Management System will be discussed in a future edition of Compact.

LITERATURE

[ANSI86] ANSI X9.9, *Financial Institution Message Authentication (Wholesale)*, 1986.

[EDIF91] EDIFORUM, *Nationale EDI Gids 91/92*, 1991.

[MD491] MD4 EDIFACT Security Group, *Security framework for EDIFACT*, Document 1.19 V 1.6, 14 March 1991.

[UN/E92] UN/EDIFACT Security Joint Working Group, *EDIFACT Security Implementation Guidelines*, 9 June 1992.

[IEEE92] IEEE, *Special report on Data Security*, IEEE Spectrum, August 1992.

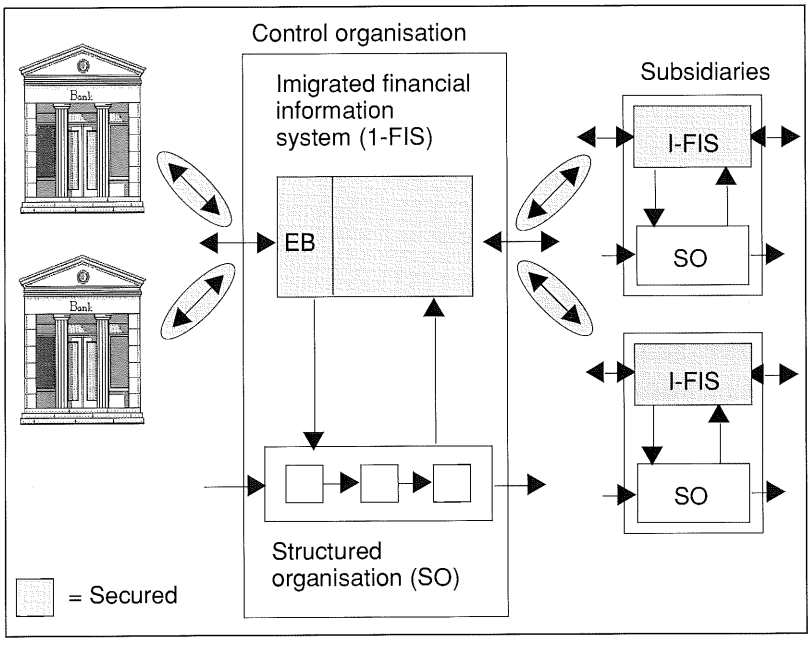
[ISO88] ISO9735, *Electronic Data Interchange for administration, commerce and transport - Application level syntax rules by the International Organisation for Standardization* (ISO). Reference number: ISO 9735: 1988 (E).

[OECD92] OECD, *Recommendation of the council concerning guidelines for the security of information systems, guidelines for the security of information systems, and explanatory memorandum to accompany the guidelines*, Ad hoc group of experts, Paris, 1992.

[UNTD91] United Nations, *United Nations Trade Data Interchange Directory (UNTDID)*, Issue 91.2. Trade/WP.4/R.740/, 1991.

[Vrie92] Drs. T.P. de Vries, *The Implementation of TSS*, Compact 1991/2.

Figure 6. Secure electronic banking as a result of the project.



H. Roos RA
Is partner of KPMG Klynveld from 1980 and since 1991 leading the technical specialists of KPMG Klynveld Management Consultants.
This group includes specialists in the field of telecommunication and networks, software engineering, documentary information systems, cryptography, information security and risk-analysis.

H. Veenman MBT
Has been involved with computers and telecommunications since 1978.
At KPMG Klynveld Management Consultants he is as a senior manager responsible for the consultancy activities in the field of telecommunications and telematics.
Within the professional field of telecommunications projects are being performed under his responsibility in the field of information security, corporate networking, network management and organisation.

Beveiligingsaspecten en juridische aspecten als communicerende vaten

Ir. G.J. Schuringa en mr. R.E. van Esch

EDI betekent een efficiënte berichtenuitwisseling tussen twee partijen. Berichten met vaak belangrijke transacties of financiële inhoud. Misbruik en fraude kunnen in deze omgeving dus veel schade aanrichten. Reden om eens nader stil te staan bij de beveiliging van dit berichtenverkeer.
In dit artikel wordt op heldere wijze ingegaan op deze beveiliging en wordt uitgebreid aandacht besteed aan de juridische aspecten die bij deze beveiliging van belang zijn.

INLEIDING

EDI kent een groot aantal aspecten. Genoemd kunnen worden organisatorische aspecten, marketing-aspecten, datacommunicatie-aspecten, software-aspecten, standaardisatie-aspecten, fiscale aspecten, accountancy-aspecten, beveiligingsaspecten en juridische aspecten. Tussen de laatste vier aspecten bestaat een zeker verband. In al deze vier deelgebieden komt de vraag aan de orde welke maatregelen er moeten worden genomen om EDI-berichten aanvaardbaar te maken als alternatief voor schriftelijke berichten. In dit artikel wordt nader ingegaan op de samenhang tussen de beveiligingsaspecten en de juridische aspecten van EDI.

DE CONNECTIES TUSSEN BEVEILIGINGSASPECTEN EN JURIDISCHE ASPECTEN

Tussen beveiligingsaspecten en juridische aspecten zijn verschillende connecties te onderkennen.

Samenhang tussen taken beveiligingsmedewerkers en juristen
Beveiligingsmedewerkers gaan uit van de potentiële bedreigingen op een systeem. Een systeem is hier een samenspel van mensen en middelen, waarbij de middelen ruim gezien moeten worden als gebouwen, hardware, software, gegevens en dergelijke. De beveiligingsmedewerkers stellen op grond van de bedreigingen beveiligingseisen op waaraan het systeem moet voldoen en werken deze uit in toe te passen beveiligingsmaatregelen. Deze beveiligingsmaatregelen zijn onderdeel van de contractuele verhouding tussen partijen.
Juristen houden zich bij het opstellen van contracten bezig met alles wat er mis kan gaan in de relatie tussen de contractpartijen. Bij het opstellen van een interchange agreement zullen zij met name aandacht besteden aan de problemen die samenhangen met de elektronische uitwisseling van berichten. Enerzijds zullen zij proberen problemen te voorkomen door ervoor te zorgen dat er in het contract en de bijlagen afspraken worden gemaakt die risico's voor partijen zoveel mogelijk vermijden. Denk bijvoorbeeld aan een bepaling in het interchange agreement waarin procedures zijn afgesproken over de ontvangstbevestiging van elektronische berichten. Wat dat betreft streven zij hetzelfde doel na als beveiligingsmedewerkers.
Anderzijds stellen juristen regelingen op voor het geval het toch mis mocht gaan. Deze taak is complementair aan de risicomijdende taak en derhalve ook complementair aan de taak van beveiligingsmedewerkers. Daarbij kan worden geconstateerd dat de noodzaak tot probleemoplossende juridische regelingen groter is naarmate er minder probleemvermijdende maatregelen worden genomen. Zo neemt het belang van een juridische regeling over de verdeling van de risico's van misbruik van cryptografische sleutels toe naarmate partijen minder beveiligingsmaatregelen hebben getroffen om zo'n misbruik te voorkomen.

Samenhang tussen beveiliging en de bewijsrechtelijke positie van een deelnemer aan een EDI-systeem
Indien bijvoorbeeld de afzender en de ontvanger van een elektronisch bericht voor de rechter twisten over de uitwisseling (is het bericht verzonden, is het bericht ontvangen) of over de inhoud van het uitgewisselde bericht, zal de rechter aan één van hen opdragen om bewijs te leveren. Voor het voldoen aan deze bewijsopdracht zal deze partij in het geschil gebruik dienen te maken van elektronische registraties of reprodukties van elektronische registraties. De rechter staat het vrij om te beoordelen welke waarde hij aan dergelijke bewijsmiddelen toekent. Bij deze beoordeling zal van groot belang zijn welke beveiligingsmaatregelen er zijn genomen om te voorkomen dat er een onjuiste registratie heeft plaatsgevonden en dat het bericht na registratie van inhoud is veranderd.

Samenhang tussen een adequate beveiliging voor een beroep op een bewijsovereenkomst
Het Nederlandse bewijsrecht is regelend recht. Het staat partijen in principe vrij om in een overeenkomst af te wijken van het bewijsrecht zoals dat in de wet is opgenomen. Zo kunnen deelnemers aan een EDI-systeem overeenkomen dat de bewijsmiddelen van één van hen dwingend bewijs opleveren tot op tegenbewijs. Dit heeft tot gevolg dat de rechter ervan moet uitgaan dat de elektronische registratie van de partij te wiens gunste de overeenkomst is gemaakt, de feiten juist weergeeft tot op tegenbewijs. De rechter heeft echter de bevoegdheid een dergelijke bewijsovereenkomst opzij te zetten indien hij meent dat deze in strijd is met de redelijkheid en de billijkheid. Dit zal hij eerder doen indien hij constateert dat het systeem van degene die zich daarop beroept, onvoldoende beveiligd is tegen onjuiste registratie van berichten en informatie over de uitwisseling of manipulatie na registratie. Er gaan zelfs stemmen op om bedrijven in hun relatie met particulieren slechts dan een beroep op een dergelijke bewijsclausule in een overeenkomst toe te staan indien zij bewezen hebben hun EDI-systeem voldoende te hebben beveiligd.

Juristen houden zich bij het opstellen van contracten bezig met alles wat er mis kan gaan in de relatie tussen de contractpartijen.

Wat in dit kader een voldoende mate van beveiliging is hangt af van de omstandigheden van het geval. Daarbij zal ten eerste een rol spelen om wat voor berichten het gaat. Zo is het belang bij het beveiligen van een financieel EDI-systeem groter dan bij een EDI-systeem voor postorderbedrijven. Voorts kan de omvang van de risico's een rol spelen bij de beslissing van de rechter.
Tot slot zal de rechter ook acht slaan op eventuele gebruiken ten aanzien van de beveiliging in de relevante branche. Kortom, de rechter zal vaststellen welke beveiligingsmaatregelen een redelijke instelling in de desbetreffende branche zou hebben genomen om het risico dat zich heeft voorgedaan, te vermijden.

Samenhang tussen een adequate beveiliging en een beroep op contractbepalingen die betrekking hebben op misbruik van het systeem
Denk bijvoorbeeld aan bepalingen aan de hand waarvan kan worden vastgesteld wie van de deelnemers aan het EDI-systeem het risico draagt, indien een onbevoegde derde al dan niet met gebruikmaking van diens identificatiemiddelen onder naam van een deelnemer een bericht verstuurt. Partijen kunnen in het interchange agreement overeenkomen dat één van hen deze risico's draagt. De rechter heeft op grond van de Nederlandse wet de bevoegdheid om een dergelijke be-

paling terzijde te zetten, indien hij deze onder de gegeven omstandigheden onredelijk en onbillijk vindt. Komt zo'n bepaling voor in de algemene voorwaarden van een onderneming, dan loopt de gebruiker van deze voorwaarde het risico dat de rechter de voorwaarde op verzoek van de wederpartij vernietigt omdat de voorwaarde onredelijk bezwarend is voor de wederpartij.
De rechter heeft deze mogelijkheid in het geval dat de wederpartij een natuurlijk persoon is of een rechtspersoon (zoals een NV of een BV) met een kleine onderneming. Bij het beantwoorden van de vraag of hij een beroep op een dergelijke contractbepaling zal toestaan, zal de rechter in de meeste gevallen aandacht schenken aan de wijze waarop het systeem is beveiligd tegen een dergelijk misbruik.

Samenhang tussen de beveiliging en de juridische gebondenheid aan een bericht
Een ontvanger van een EDI-bericht loopt altijd het risico dat de vermeende afzender ontkent dat het bericht van hem afkomstig is. In dat geval berust in beginsel op de ontvanger de last het tegendeel te bewijzen. Bij het ontbreken van een schriftelijke handtekening onder het bericht zal hij aan de hand van het in het bericht gebruikte identificatiemiddel dit bewijs moeten leveren. Naarmate de gebruikte identificatie- en authenticatiemethode beter beveiligd is tegen misbruik door onbevoegde derden, zal de rechter eerder aannemen dat het bericht afkomstig is van de deelnemer aan het EDI-systeem bij wie het gebruikte identificatiemiddel hoort. Ook is het mogelijk dat de rechter in dat geval de bewijslast omdraait en de vermeende afzender de opdracht geeft te bewijzen dat het bericht niet van hem afkomstig is.

Een ontvanger van een EDI-bericht loopt altijd het risico dat de vermeende afzender ontkent dat het bericht van hem afkomstig is.

Overigens zou het probleem ook juridisch kunnen worden opgelost doordat partijen contractueel overeenkomen dat misbruik van een identificatiemiddel van één van de deelnemers voor rekening van deze deelnemer komt. Daarbij dient echter te worden opgemerkt dat de rechter een beroep op een dergelijke bepaling kan afwijzen omdat dit onder de gegeven omstandigheden in strijd is met de redelijkheid en de billijkheid. De kans hierop is groter indien degene die zich op een dergelijke bepaling beroept, het systeem heeft ontworpen en beheert en onvoldoende maatregelen heeft genomen om het te beveiligen tegen onbevoegd gebruik van identificatiemiddelen.

DE PLAATS VAN DE BEVEILIGINGSBEPALINGEN IN HET INTERCHANGE AGREEMENT

De inhoud van een interchange agreement kan grofweg worden onderverdeeld in drie categorieën:
a. de technische onderwerpen;
b. de beveiligingsonderwerpen;
c. de juridische onderwerpen.

Bij de technische onderwerpen kan men denken aan afspraken over te gebruiken communicatieprotocollen, berichtenstandaarden, etc.
De juridische onderwerpen omvatten onder andere bewijs, tijdstip en plaats van totstandkoming van de overeenkomst, privacy-aansprakelijkheid, toepasselijk recht en bevoegde rechter.

De bepalingen met betrekking tot de beveiliging zijn naar hun aard probleemvermijdende bepalingen (zie voorgaande paragraaf). Het betreffen over het algemeen kaderbepalingen. Partijen spreken af dat zij beveiligingsmaatregelen zullen nemen om te voorkomen dat bepaalde met name genoemde risico's zich zullen voordoen. De nadere uitwerking van de te nemen maatregelen vindt plaats in de bijlagen bij het contract.

In deze beveiligingsbepalingen komt het samenspel tussen juristen en beveiligingsmedewerkers bij de vervulling van hun taak tot het vermijden van problemen duidelijk naar voren. In eerste instantie zullen de beveiligingsmedewerkers een risico-analyse moeten maken. Daarbij zullen zij aandacht moeten besteden aan de aard van het risico dat zij door de beveiliging trachten te verminderen, de kans dat dit risico zich voordoet, de mogelijke schadelijke gevolgen bij het zich verwezenlijken van het risico en de omvang van de mogelijke schade. Het risico kan zich vertalen in een financieel risico of een immaterieel risico zoals het schaden van de goede naam. Voor wat dit laatste betreft kan bijvoorbeeld worden gedacht aan het bekend worden van medische gegevens afkomstig van een zorgverzekeraar. Vervolgens zullen zij moeten aangeven welke maatregelen er kunnen worden genomen om het EDI-systeem tegen dergelijke risico's te beschermen en welke kosten daaraan zijn verbonden.
Aan de hand van deze gegevens zal op beleidsmatig niveau dienen te worden beslist welke maatregelen er uiteindelijk zullen worden genomen. Bij het nemen van deze beleidsbeslissing zal tevens een rol spelen welke invloed het al dan niet toepassen van bepaalde beveiligingsprocedures heeft op de juridische positie van de instelling. Voorts zullen de kosten een belangrijke rol vervullen in het besluitvormingsproces. Gebruikers van EDI zullen bij het beantwoorden van de vraag of zij beveiligingsmaatregelen zullen nemen en de mate waarin zij beveiligingsmaatregelen zullen nemen deze kosten dienen af te wegen tegen de voordelen die zij daarvan hebben.
Tot slot is het aan de juristen om, nadat de beleidsbeslissingen zijn genomen, een en ander in een juridisch kader vast te leggen.

DE BEVEILIGINGSBEPALINGEN IN EEN INTERCHANGE AGREEMENT

In een interchange agreement wordt over het algemeen ruim aandacht besteed aan de beveiligingsaspecten. De regelingen die men over dit onderwerp tegenkomt kan men onderverdelen in de volgende categorieën:
- systeembeveiliging;
- berichtenbeveiliging;
- uitwisselingsbeveiliging.

Systeembeveiliging

Deze beveiliging ziet op het totale EDI-systeem, waaronder kunnen worden gerekend het computersysteem van de afzender, van de ontvanger, van een ingeschakelde intermediair en het datacommunicatienetwerk. Zij wordt gerealiseerd door fysieke en logische beveiliging. Zij heeft tot doel te voorkomen dat onbevoegde derden zich toegang verschaffen tot het systeem en kennis nemen van daarin opgeslagen berichten, deze berichten van inhoud veranderen of vernietigen, dan wel onbevoegdelijk berichten versturen.

Hieromtrent bepaalt de EDIFORUM EDI-overeenkomst in artikel 6.1 het navolgende:
Partijen verbinden zich tot het implementeren en in stand houden van controle- en beveiligingsprocedures en maatregelen om de bescherming van berichten tegen risico's van ongeautoriseerde toegang, verlies of vernietiging zeker te stellen.

Deze bepaling legt slechts de verplichting aan partijen op procedures en maatregelen te nemen. De nadere uitwerking van de procedures en maatregelen wordt aan de individuele partijen overgelaten. Gedacht kan worden aan de volgende procedures en maatregelen:
- het toepassen van een authenticatiemethode voor alle berichten;
- het toepassen van een methode om de integriteit van de berichten(stroom) te bewaken;
- het toepassen van een methode om de vertrouwelijkheid van de berichten te waarborgen;
- het toepassen van toegangsbeperkende systemen tot de computerruimten, waardoor alleen de bevoegde medewerkers toegang hebben en alle anderen worden geweerd;
- het toepassen van logische toegangssystemen tot de computers en terminals waardoor alleen geïdentificeerde gebruikers díe systeemfuncties kunnen toepassen waarvoor zij geautoriseerd zijn;
- het hebben van een uitwijkplan, waardoor bij het uitvallen van de eigen computerverwerking binnen een vast te stellen tijd in uren de verwerking op een ander computersysteem weer kan worden opgestart,

maar eventueel ook:
- het toepassen van compartimentering van de computerruimten, waardoor de belangrijkste systeemfuncties slechts door een nog beperktere groep medewerkers kunnen worden uitgevoerd;
- het beschikken over een door de hoogste leiding goedgekeurd beveiligingsbeleid, waarin de verantwoordelijkheden voor en de organisatie van de beveiliging zijn geregeld;
- het toepassen van geheimhoudingsverklaringen voor medewerkers ten aanzien van de EDI-berichten;
- bij vermeende onregelmatigheden, zoals veel grotere bestelling dan gewoonlijk, een ander afleveradres of een ongebruikelijke bestelling, direct de andere partij informeren.

De juridische waarde van deze bepaling doet zich bijvoorbeeld gelden in het geval dat er door een onbevoegde derde misbruik van het systeem wordt gemaakt. Mocht blijken dat dit mogelijk is geweest omdat één van de partijen zijn systeem niet of onvoldoende heeft beveiligd tegen ongeautoriseerde toegang, dan zal de rechter bij het beantwoorden van de vraag wie de schade moet dragen zeker rekening houden met de afspraken neergelegd in artikel 6.1.

Berichtenbeveiliging

Voor het realiseren van beveiliging op berichtenniveau kan worden gebruik gemaakt van encryptietechnieken. Het doel is de authenticiteit, de vertrouwelijkheid en de integriteit van het bericht te bewaren.

De EDIFORUM EDI-overeenkomst bepaalt in artikel 6.3 hieromtrent het volgende:
Om beveiligingsredenen kunnen partijen overeenkomen om een specifieke beveiligingsvorm, zoals encryptie of een andere tussen partijen overeengekomen methode, te gebruiken voor bepaalde berichten, indien en voor zover de wet zulks toestaat. Dezelfde methode zal worden gebruikt voor iedere daarop volgende transmissie of retransmissie van een beveiligd bericht.

De beveiligingsmaatregelen in de EDIFACT-berichten zijn gebaseerd op versleutelingsmethoden met geheime sleutels. De meest toegepaste versleutelingsmethoden zijn DES en RSA.
De oudste is Data Encryption Standard (DES). DES gebruikt een geheime sleutel die voor de verzender en de ontvanger van een bericht hetzelfde is. DES is een zogenaamd symmetrisch algoritme, een rekenmodel waarbij zowel de versleuteling als de ontsleuteling met een zelfde sleutel plaatsvindt. DES kan berichten encrypten om de vertrouwelijkheid te bewaken, alsook voorzien van een elektronische handtekening om de authenticiteit van de bron van het bericht te garanderen.
Bij het gebruik van een symmetrisch algoritme zoals DES is de beveiligde distributie van de geheime sleutel van groot belang.

RSA, genoemd naar zijn uitvinders Rivest, Shamir en Adleman, is een asymmetrisch algoritme. RSA hanteert twee verschillende sleutels: een geheime en een openbare sleutel. De geheime sleutel houdt de eigenaar echt geheim, maar de openbare sleutel stelt hij aan zijn zakenrelaties ter beschikking. De verzender van een bericht kan met behulp van zijn

geheime sleutel het bericht voorzien van een elektronische handtekening. De ontvanger van het bericht kan met de openbare RSA-sleutel van de verzender de elektronische handtekening van de verzender verifiëren. Met de openbare sleutel van de ontvanger van het bericht kan de verzender een bericht encrypt verzenden. Alleen de ontvanger van het bericht kan met zijn geheime RSA-sleutel het encrypte bericht weer in leesbare tekst omzetten.
Bij het gebruik van een asymmetrisch algoritme zoals RSA is het authenticeren van iemands openbare RSA-sleutel van groot belang.

Indien de openbare RSA-sleutel van de verzender van een bericht niet geauthenticeerd (gewaarmerkt) is, kan een ieder zich voordoen als "de verzender" door naar de ontvanger zijn openbare RSA-sleutel op te sturen.

Indien partijen besluiten encryptietechnieken toe te passen, zullen zij afspraken moeten maken over het sleutelbeheer.

Het authenticeren van een openbare RSA-sleutel gebeurt door een Certificatie Autoriteit (CA). Deze CA is een door partijen vertrouwde instantie. De CA stelt eerst onomstotelijk de authenticiteit van de eigenaar van de openbare RSA-sleutel en de integriteit van de sleutel vast. Vervolgens versleutelt de CA de openbare RSA-sleutel te zamen met onder andere de naam van de eigenaar met behulp van zijn eigen geheime RSA-sleutel. Dit heet het certificaat van de openbare RSA-sleutel van de eigenaar. De openbare RSA-sleutel van de CA is voor een ieder ter beschikking. Met deze CA-sleutel, het RSA-algoritme en het certificaat kan vervolgens een ieder de authenticiteit van de eigenaar van een openbare RSA-sleutel, gecertificeerd door deze CA, onomstotelijk vaststellen.

Indien partijen besluiten encryptietechnieken toe te passen, zullen zij afspraken moeten maken over het sleutelbeheer. Daarbij kunnen de volgende aspecten aan de orde komen:
- bepalen wie de sleutel vaststelt;
- bepalen op welke wijze de sleutel aan de andere partij wordt bekend gemaakt;
- bepalen op welke wijze de sleutel wordt bewaard;
- bepalen hoe de cryptografische bewerkingen worden uitgevoerd;
- een procedure vaststellen voor regelmatige vernieuwing van de sleutel om de kans op misbruik te verkleinen;
- vaststellen welke medewerkers bevoegd zijn de sleutel te gebruiken;
- een procedure vaststellen voor tussentijdse wijziging, bijvoorbeeld bij diefstal van de security box waarin de geheime sleutel is opgeslagen;
- een procedure vaststellen voor het geval dat wordt geconstateerd dat er misbruik is gemaakt van een sleutel. Hierbij kan worden gedacht aan de tussentijdse vernieuwing van de sleutel en het opzetten van een misbruikmeldpunt.

Methoden om berichten te beveiligen zijn:

- Het toevoegen van een Message Authentication Code (MAC) aan een bericht. De internationale standaard maakt gebruik van het DES-algoritme.
Dit werkt als volgt:
Het bericht wordt in delen met een standaardlengte opgesplitst. Het DES-algoritme versleutelt deze delen met een geheime sleutel. Na een sommering van de tussenresultaten wordt, om het kraken van de geheime sleutel te voorkomen, slechts de helft van de uitkomst als MAC verzonden. De ontvanger voert een zelfde berekening met een zelfde geheime sleutel uit en vergelijkt vervolgens zijn resultaat met de tegelijk met het bericht ontvangen MAC.
Bij overeenstemming van de berekende en ontvangen MAC stelt de ontvanger van het bericht vast dat het bericht is verzonden door de partij die over dezelfde geheime sleutel beschikt en dat het bericht ongewijzigd is ontvangen.
De beveiligingsmaatregel MAC realiseert de beveiligingsfuncties: authenticatie van de bron en integriteit van een bericht. Door het geven van een uniek nummer aan het bericht is tevens de berichtenvolgordebewaking gerealiseerd.

- Het zetten van een digitale handtekening onder het bericht. Hiervoor wordt het asymmetrisch algoritme RSA gebruikt.
Een digitale handtekening van een bericht is de versleutelde hash-waarde van een bericht.
Hashing geeft een berichtverkorting en is nodig omdat een RSA-versleuteling in vergelijking met DES traag werkt. Voor de hashing wordt meestal DES met een openbare DES-sleutel gebruikt. De verzender versleutelt de hash-waarde met zijn geheime RSA-sleutel en voegt dit resultaat als digitale handtekening aan het bericht toe.
De ontvanger van het bericht versleutelt de digitale handtekening met de openbare RSA-sleutel van de verzender. Vervolgens vergelijkt hij dit resultaat met de hash-waarde verkregen door hashing van het bericht op dezelfde wijze met dezelfde openbare DES-sleutel.
Bij overeenstemming van de twee resultaten stelt de ontvanger van het bericht vast dat het bericht *onloochenbaar* is verzonden door de partij waarvan hij de openbare RSA-sleutel heeft en dat het bericht ongewijzigd is ontvangen.
De beveiligingsmaatregel digitale handtekening realiseert de beveiligingsfuncties: non-repudiation en authenticatie van de bron en integriteit van een bericht. Door het geven van een uniek nummer aan het bericht is tevens de berichtenvolgordebewaking gerealiseerd.

- Het encrypten van het gehele bericht waardoor de vertrouwelijkheid van het bericht wordt gewaarborgd. Deze encryptie en decryptie vindt meestal plaats met DES.

Dit werkt als volgt:
Het bericht wordt opgesplitst in delen van gelijke lengte en vervolgens volledig encrypt met de geheime DES-sleutel.
Daar echter encryptie alle mogelijke bitpatronen kan opleveren en EDIFACT slechts een beperkte tekenset toestaat zal bij het toepassen van de benodigde filterfunctie de lengte van het bericht verdubbeld worden.
De ontvanger van het bericht zal eerst de omgekeerde filterfunctie uitvoeren en vervolgens het bericht met een zelfde geheime DES-sleutel decrypten.
Na de decryptie weet de ontvanger echter niet of hij het bericht ongewijzigd heeft ontvangen. Daartoe heeft hij altijd additioneel een MAC of digitale handtekening nodig.
De beveiligingsmaatregel encryptie realiseert de beveiligingsfunctie: vertrouwelijkheid.

Deze bepaling is bedoeld om partijen eraan te herinneren dat er de mogelijkheid bestaat afspraken te maken omtrent beveiliging op berichtniveau. De verplichting tot een dergelijke beveiliging vloeit niet voort uit artikel 6.3 zelf maar uit de eventuele nadere afspraken die partijen daaromtrent maken. Worden dergelijke afspraken gemaakt, dan zal de niet-nakoming daarvan door één van de partijen tot gevolg kunnen hebben dat hij het risico draagt van manipulatie van de inhoud van het bericht tijdens transport over het netwerk.

Uitwisselingsbeveiliging

De uitwisselingsbeveiliging betreft de technieken die de afzender en de ontvanger middelen verschaffen om te controleren en vast te stellen wie hun wederpartij is bij de uitwisseling. Het gaat om onderwerpen als identificatie, authenticatie en non-repudiation.

De EDIFORUM EDI-overeenkomst bepaalt daaromtrent in artikel 6.2 het navolgende:
In aanvulling op de in UN/Edifact voorziene controle-elementen, die voor EDI-berichten van belang zijn, dienen partijen procedures of methoden, die de verificatie van berichten waarborgen, overeen te komen. Verificatie van berichten sluit in de identificatie, de authenticatie en de verificatie van de integriteit van het bericht en de herkomst van het bericht door het gebruik van een authenticatiemiddel zoals een gedigitaliseerde handtekening en/of beveiligingsmiddel of procedure om vast te stellen dat een bericht echt is. De specificaties met betrekking tot de berichtverificatie zullen worden vastgelegd in de Technische Bijlage.

In het geval dat berichtverificatie leidt tot een verwerping van het bericht of de ontdekking van een fout in het bericht, zal de ontvanger de afzender daarvan in kennis stellen binnen de tijdlimieten die zijn vastgelegd in de Technische Bijlage of door partijen zijn overeengekomen, mits de afzender is geïdentificeerd, en zal de ontvanger niet handelen op het bericht voordat de afzender hem heeft geïnstrueerd om dit te doen.

De volgende methoden kunnen worden gebruikt voor de identificatie en de authenticatie van het bericht:
- het toepassen van een DES MAC;
- het toepassen van een digitale handtekening.

Non-repudiation houdt in dat er technieken worden gebruikt waardoor de afzender niet kan ontkennen dat het bericht van hem afkomstig is en de ontvanger niet kan ontkennen dat hij het bericht daadwerkelijk heeft ontvangen. Aan de volgende methode(n) kan worden gedacht:

- Het toepassen van een digitale handtekening door de verzender met RSA, waardoor naast de bronauthenticatie en de integriteitsbewaking van het bericht tevens non-repudiation of origin wordt gerealiseerd. Immers, alleen de eigenaar van de geheime sleutel kan zijn digitale handtekening zetten, terwijl een ieder die over de bijbehorende openbare sleutel beschikt de handtekening kan verifiëren.

- De beveiligingsfunctie: het niet kunnen loochenen van de ontvangst en de inhoud van een bericht door de ontvanger (non-repudiation van ontvangst) is alleen te realiseren met behulp van een apart bericht omdat dit pas kan worden aangemaakt nadat alle controles op het ontvangen bericht zijn uitgevoerd. Hierbij zet de ontvanger een eigen digitale handtekening met zijn eigen geheime RSA-sleutel over de ontvangen digitale handtekening en zendt deze naar de verzender van het bericht.

Dit artikel is door de auteurs geschreven in opdracht van de Stichting EDIFORUM te Leidschendam en is reeds eerder gepubliceerd als een hoofdstuk in de EDI Gids 92/93. De EDI Gids is een jaarlijkse uitgave van de Stichting EDIFORUM.

Ir. G.J. Schuringa
Is information security officer van de Produktgroep Betaaldiensten van Rabobank Nederland. Hij is onder andere lid van de Security Joint Working Group van WP4 van de UN/ECE.

Mr. R.E. van Esch
Is senior jurist van de Juridische en Fiscale dienst van Rabobank Nederland en universitair hoofddocent van de Sectie Recht en Informatietechnologie van de Rijksuniversiteit Utrecht. Hij is onder andere lid van de Working Group on legal aspects of EDI van de ICC en van het Legal Rapporteurs team van WP4 van de UN/ECE.

EDP AUDITORIUM

ONTWERP-AANBEVELING INFORMATIE-BEVEILIGING

Mw. ir. T.D. de Haan

Recommendation of the council concerning guidelines for the security of information systems,
guidelines for the security of information systems,
and
explanatory memorandum to accompany the guidelines.

Ad hoc group of experts on guidelines for the security of information systems, Committee for Information, Computer and Communications Policy, Directorate for Science, Technology and Industry, Organisation for Economic Co-operation and Development.

DSTI/ICCP/AH(90)21/REV6, PARIS, 1992.

Inleiding

In maart 1990 is door het Committee for Information, Computer and Communications Policy van de Organisation for Economic Co-operation and Development (OECD) een werkgroep opgericht om richtlijnen voor informatiebeveiliging op te stellen. De activiteiten van deze werkgroep, bestaande uit experts op het gebied van informatiebeveiliging, hebben geresulteerd in een ontwerp-aanbeveling informatiebeveiliging.

Achtergrond

Het gebruik van computers is in de loop der jaren sterk toegenomen en steeds meer geïntegreerd en geaccepteerd in onze samenleving. Informatiesystemen zijn een vitaal onderdeel geworden van het functioneren van regeringen, organisaties en individuen. Een informatiesysteem is een complex geheel van computers, communicatiefaciliteiten en (lokale) communicatienetwerken. Het uiteindelijke doel van een dergelijk informatiesysteem is het opslaan, verwerken en verzenden van informatie. De afhankelijkheid van informatiesystemen is hierdoor eveneens sterk toegenomen en neemt nog steeds toe. Vergeleken met papieren documenten is de informatie in informatiesystemen extra kwetsbaar.
De toenemende afhankelijkheid en kwetsbaarheid van informatiesystemen heeft tot gevolg dat een betere beveiliging noodzakelijk is. Men moet zich hiervan bewust worden en maatregelen nemen om de risico's te verkleinen. Een betere beveiliging is ook noodzakelijk om het vertrouwen van de gebruikers te krijgen en te behouden. Bij een gebrek aan vertrouwen door de gebruikers zullen de technologische mogelijkheden niet optimaal kunnen worden benut.
De beveiliging van de systemen blijft echter achterlopen bij de overige technologische ontwikkelingen. Het streven is om richtlijnen vast te leggen die een betere internationale samenwerking en coördinatie bevorderen, en die tegelijkertijd niet in strijd zijn met de regelgeving op nationaal niveau.

Richtlijnen voor informatiebeveiliging

De richtlijnen voor informatiebeveiliging zijn bedoeld voor de publieke en private sector en zijn van toepassing op alle soorten informatiesystemen. De belangrijkste doelstellingen van de richtlijnen zijn:
- het initiëren van een bewustwordingsproces met betrekking tot de risico's van het onvoldoende beveiligen van informatie;
- het creëren van een netwerk ter ondersteuning van degenen die in de publieke en private sector verantwoordelijk zijn voor informatiesystemen en het bevorderen van samenwerking tussen deze twee sectoren;
- het bevorderen van internationale samenwerking op het gebied van informatiebeveiliging.

De door de werkgroep gehanteerde definities zijn:

- *data:*
een representatie van feiten, concepten of instructies op geformaliseerde wijze weergegeven en bruikbaar voor communicatie, interpretatie of machinale of handmatige verwerking;

- *informatie:*
de betekenis die wordt toegekend aan de data;

- *informatiesysteem:*
computers, communicatiefaciliteiten, communicatienetwerken en informatie die hierdoor kan worden opgeslagen, verwerkt, verkregen of verzonden, alsmede de programma's, specificaties en procedures die nodig zijn voor het gebruik en onderhoud;

- *beschikbaarheid:*
de eigenschap dat data, informatie en informatiesystemen op de gewenste tijdstippen toegankelijk en bruikbaar zijn voor bepaalde personen;

- *vertrouwelijkheid:*
de eigenschap dat data en informatie alleen op geautoriseerde tijdstippen en op een geautoriseerde manier toegankelijk zijn voor geautoriseerde personen, entiteiten en processen;

- *integriteit:*
de eigenschap dat data en informatie accuraat en compleet zijn en blijven.

De beveiliging van informatiesystemen heeft tot doel de beschikbaarheid, de vertrouwelijkheid en de integriteit van de informatiesystemen te bewaken. Er wordt met betrekking tot de richtlijnen van een aantal principes uitgegaan.

Allereerst dienen verantwoordelijkheden van eigenaars, gebruikers en andere betrokkenen expliciet te zijn vastgelegd. Verder is het van belang dat eigenaars, gebruikers en andere betrokkenen op de hoogte worden gehouden van beveiligingsmaatregelen, zodat ze vertrouwen krijgen in de informatiesystemen.
Het niveau van beveiliging dient te worden aangepast aan de behoefte en mogelijkheden (bijvoorbeeld financiële en technische mogelijkheden). De beveiliging van informatie dient multidisciplinair te worden benaderd en dient een geïntegreerd geheel te zijn in de organisatie. Vanwege de veranderingen die een informatiesysteem in de loop van de tijd ondergaat is het noodzakelijk dat de beveiliging periodiek wordt geëvalueerd.
De informatiebeveiliging dient op een wijze te worden uitgevoerd die niet in strijd is met het recht op informatie.
Uiteindelijk zullen het de regeringen, ondernemingen en instanties zijn die stappen moeten zetten om een adequate informatiebeveiliging te kunnen bewerkstelligen. Hierbij realiseert de werkgroep zich dat regeringen zich niet in alle gevallen aan de richtlijnen kunnen of willen houden.

Implementatie

Het is noodzakelijk dat er wereldstandaarden worden vastgelegd voor beveiliging en voor beoordeling van systemen en produkten. Deze standaarden zouden moeten worden ontwikkeld in samenwerkingsverband tussen regeringen, normalisatie-instituten, leveranciers en gebruikers van informatiesystemen. Hierbij moet rekening worden gehouden met het feit dat deze standaardisatie maar tot een beperkt niveau kan worden doorgevoerd.
Er wordt gestreefd naar een situatie waarbij elektronische documenten bij een transactie hetzelfde vertrouwen en dezelfde juridische status hebben als papieren documenten. Hiertoe dient de huidige regelgeving te worden uitgebreid.
Afgezien van beveiliging zijn er ook andere maatregelen denkbaar om informatiesystemen te beschermen, namelijk sancties. Om effectief te kunnen zijn dienen deze sancties op internationaal niveau te worden geregeld. Hiermee is al een begin gemaakt. Een groot probleem is echter de verschillende wetgeving in de individuele landen.
Opleiding kan een belangrijke bijdrage leveren tot de bewustwording van de noodzaak tot het beveiligen van informatiesystemen. Hier ligt een taak voor zowel regeringen als ondernemingen.

Bedreigingen

Het functioneren van een informatiesysteem kan worden beïnvloed door technologische ontwikkelingen, technische problemen, omgevingsfactoren, menselijke fouten en/of sociale, politieke en economische ontwikkelingen. Het niet naar behoren functioneren van een informatiesysteem kan directe financiële schade tot gevolg hebben. Ook kan er niet direct aanwijsbare schade ontstaan, bijvoorbeeld het verloren gaan van persoonsgegevens of andere gevoelige informatie.

De technische oorzaken van het niet goed functioneren van een informatiesysteem kunnen liggen in een interne of externe systeemcomponent of kunnen opzettelijk zijn, zoals computervirussen. Omgevingsfactoren kunnen worden onderverdeeld in natuurrampen zoals aardbevingen, en kleine storingen zoals lekkage en stroomstoring.
Het streven is om standaarden voor de beveiliging te ontwerpen. Een probleem echter bij het implementeren van een adequate beveiliging is dat er diverse leveranciers zijn. Een ander probleem bij de beveiliging van informatiesystemen is dat er rekening moet worden gehouden met de diverse achtergronden van de betrokkenen. Operators en gebruikers dienen voldoende opleiding en instructies te krijgen om de risico's te beperken. Maar zelfs met voldoende opleiding en instructies kunnen werknemers opzettelijk fraude en dergelijke plegen. Procedures om dit te voorkomen beslaan een breder terrein dan alleen de computers.
Belangrijk is dat de kosten van beveiliging in verhouding staan tot de baten. Dit geldt zowel voor de eigenaar van de informatiesystemen als voor degenen die eventueel deze beveiliging willen doorbreken.

Conclusie

Het uitbrengen van deze ontwerp-richtlijn informatiebeveiliging onderstreept de toegenomen aandacht voor bedreigingen van toepassingen van informatietechnologie en de noodzaak daartegen maatregelen te treffen. Na initiatieven van onder andere het Amerikaanse Department of Defense (Orange book, 1983) en de Commissie van de Europese Gemeenschappen (Information Technology Security Evaluation Criteria (ITSEC), 1991) heeft nu ook de OECD zich in de discussie gemengd.
Het is van belang dat de verschillende initiatieven op elkaar worden afgestemd. De OECD roept de lidstaten op maatregelen te treffen die een afspiegeling vormen van de richtlijnen in de aanbeveling, en om in internationaal verband standaarden te ontwikkelen voor de beveiliging van informatiesystemen. Aanzetten voor dergelijke standaarden zijn voorhanden met de Amerikaanse Trusted Computer System Evaluation Criteria en de Europese ITSEC. Zij kunnen worden gebruikt voor het meetbaar maken van informatiebeveiliging. De rol van de overheid is om - zo dat in het publiek belang is - met een sanctiebeleid een voldoende niveau van informatiebeveiliging af te dwingen.

CUMULATIEF

Overzicht van eerder verschenen artikelen in Compact

Een selectie van geactualiseerde artikelen uit de 12 1/2 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.

3 18e jaargang 91/3 herfst 1991

Beveiligingsbeleid geautomatiseerde informatievoorziening
mw. D. Jansen Heijtmajer

Geautomatiseerde produktiebesturing
E.J.M. Ridderbeekx

Audit van CA-SEVEN
E.J.M. Ridderbeekx

Registratie en analyse van produktieproblemen
ing. J.R. Hendriks en drs. J. Kuipers RA

SAP en de beheersing van geautomatiseerde controles
A.A.J. Breed RI, M. Groesz RI en drs. M.A. Weverink

4 18e jaargang 91/4 winter 1991

Systemen voor logische toegangsbeveiliging
drs. P. Veltman RA

Toepassing van CA-ACF2 in de praktijk
ing. D.J. Huis

Access control op Unisys A Serie computers
drs. M.A. Bongers RA en J-M. van Leerdam

Beveiliging van Tandem-systemen
K.E.A. van Dijk en M.M.J.A. van Dijk

RACF als access control software voor MVS-omgevingen
ing. G.H.M. Meijer

Implementatie van een beveiligingspakket
J.H. Diekema

1 19e jaargang 92/1 lente 1992

Fysieke beveiliging, een overzicht
J.F.C. van Epen CISA

Water en vuur. Effectiviteit van brandbeveiligingsmaatregelen in en om rekencentra
ing. J.F. Kuperus en ing. G.H.M. Meijer

Netconditionering
R. van de Wouw

Fysieke beveiliging en de chipcard-technologie
drs. Th.H. van Hesteren, ing. J.A.M. van Schaik en drs. T.P. de Vries

Beveiligingsbeleid gegevens en gegevensverwerking, een praktisch voorbeeld
ir. B.J.M. van Wely

Forensische EDP-auditing
R.A. s'Jacob RA

2 19e jaargang 92/2 zomer 1992

Investeren in informatietechnologie:
take IT or leave IT
drs.ing. G.J.P. Swinkels en drs. H.G.P. van Irsel

Managing with Information Technology
- a decade of wasted money?
ir. M.C.A. van Nievelt

Informatietechnologie in een kantooromgeving: produktiviteitsmanagement van kantoorarbeid en kantoorautomatisering
drs. F.R.E. Lekanne Deprez

Het plannen en rechtvaardigen van infrastructurele IT-investeringen
drs. H.G.P. van Irsel en P. Fluitsma

Uitbesteding van automatisering:
more than make or buy
mw. drs. H.W.A. van den Heuvel en mw. mr. A.M.Ch. Kemna MBA

3 19e jaargang 92/3 herfst 1992

De EDI-infrastructuur bij de Kas-Associatie
P. van Berge

Beheersbaarheid van het EDI-verkeer in de praktijk
G.J. Endenburg RI

EDI bij de Rijksdienst voor het Wegverkeer
J.W.J. Laan

EDI, een strategisch perspectief voor het bankwezen
drs. M.A. Bongers RE en mw.drs. M. Steeman

Beheersing van inzet en gebruik IT:
van kopzorg tot hoofdzaak
drs. G.C.M. Mol en drs. J.F.H. Vrins