(19) Bureau voor de Industriële Eigendom Nederland

(11) **1003644**

(12) C **OCTROOI**[20]

(21) Aanvrage om octrooi: **1003644**

(22) Ingediend: **19.07.1996**

(51) Int.Cl.[7]
H04L9/32, H04L29/06

(30) Voorrang:
19.07.1995 US 503984

(41) Ingeschreven:
21.01.1997 I.E. 1997/03

(47) Dagtekening:
11.01.2000

(45) Uitgegeven:
01.03.2000 I.E. 2000/03

(73) Octrooihouder(s):
Premenos Corp. te Concord, Californië, Verenigde Staten van Amerika (US).

(72) Uitvinder(s):
Lew Jenkins te Pleasant Hill, Californië (US)
Emmanuel Kuan Pasetes Jr. te Danville, Californië (US)

(74) Gemachtigde:
Mr. G.L. Kooy c.s. te 2514 BB Den Haag.

(54) **Werkwijze en systeem voor het verschaffen van veilige edi over een open netwerk.**

(57) Een werkwijze en systeem voor het selectief verbinden van een groot aantal computers over een open publiek netwerk, zoals het Internet, verschaft een privé veilige computeruitwisseling van EDI uitwisselingscommunicaties tussen een zendcomputer en een ontvangcomputer, elk waarvan een geassocieerde publieke sleutel en een geassocieerde privé sleutel heeft, zoals in een RSA type cryptografisch communicatiesysteem. Het geassocieerde EDI bevestigingsbericht, zoals het AUTACK, wordt gebruikt om veilige authenticatie en niet-afwijzing van zowel oorsprong als de ontvangst van de veilige privé EDI uitwisselingscommunicaties verzonden over het open publieke netwerk te verschaffen waarbij het AUTACK verzonden van de zendcomputer digitaal ondertekend is met de privé sleutel van de zender, en waarbij het antwoord AUTACK verzonden van de ontvangcomputer digitaal ondertekend is met de privé sleutel van de ontvanger. De respectieve digitaal ondertekende AUTACK's worden na ontvangst gedecodeerd door het gebruiken van de publieke sleutel geassocieerd met de privé sleutel die gebruikt wordt om de digitale ondertekening te verschaffen. Het verzonden AUTACK van de zendcomputer bevat een MD5 voor de gehele EDI uitwisseling alsmede een MD5 van het AUTACK, waarbij het AUTACK, aldus, gebruikt wordt om de digitale ondertekening te verschaffen. Het antwoord AUTACK van de ontvangcomputer omvat een MD5 van het antwoord AUTACK. De mogelijkheid om zaken te doen over het netwerk wordt geregeld door privé handelspartnersovereenkomstcommunicaties die sleutelcertificatie verschaffen.

NL C 1003644

De inhoud van dit octrooi komt overeen met de oorspronkelijk ingediende beschrijving met conclusie(s) en eventuele tekeningen.

WERKWIJZE EN SYSTEEM VOOR HET VERSCHAFFEN VAN VEILIGE EDI OVER EEN OPEN NETWERK

Achtergrond van de uitvinding

Gebied van de uitvinding

De onderhavige uitvinding heeft betrekking op werkwijzen en systemen voor het verschaffen van veilige EDI over een open systeemnetwerk, zoals het INTERNET, en in het bijzonder op een verbeterde werkwijze en systeem voor het verschaffen van een veilig EDI bericht over een open netwerk dat een RSA type publieke/privé sleutel coderingsschema gebruikt teneinde veilige authenticatie en niet-afwijzing van zowel oorsprong als ontvangst af te geven.

Publieke/privé sleutel veilige communicatiesystemen over een open netwerk zijn bekend, zoals beschreven in de Amerikaanse octrooischriften 4.578.531, 4.471.164, 5.268.962, 5.142.577, 4.893.338, 5.222.140, 5.261.002, 5.073.934, 5.303.303, 5.297.208, 5.369.705, 5.351.293, 5.375.169, 5.224.166, 5.253.294 en 5.237.611. Het RSA publieke/privé sleutel coderingsschema, is een bekend publiek sleutelsysteem voor het verschaffen van veilige berichten over een open netwerk, zoals het INTERNET, en is beschreven in verscheidene verleende Amerikaanse octrooischriften, zoals de Amerikaanse octrooischriften 4.405.829, 4.424.414, 4.200.770, 4.218.582, 5.073.935 en 4.723.284, de inhoud waarvan hierin opgenomen is door verwijzing. Bovendien is het concept van niet-afwijzing van oorsprong bekend, zoals beschreven in de Amerikaanse octrooischriften

5.226.709 en 5.367.573; alsmede dergelijke systemen waarin digitale ondertekeningen gebruikt worden in publieke/privé sleutel systemen, zoals beschreven in de Amerikaanse octrooischriften 5.311.591; 5.214.702; 5.337.360; 4.868.877; 5.001.752; 5.005.200; 5.136.643; 5.018.196; 4.885.777; 4.267.782; 5.351.302; 5.208.858; 5.299.263; 5.142.578; 4.987.593; 4.991.210; 5.339.361; 5.373.558; 4.625.076 en het Entrust systeem verhandeld door Northern Telecom. Bovendien zijn verscheidene andere veilige transmissie systemen ontwikkeld in de jaren in een poging om veilige zakencommunicaties over publieke of privé netwerken te verschaffen, zoals beschreven in de Amerikaanse octrooischriften 5.369.702, 4.876.716, 5.199.074, 4.823.388, 5.268.962, 5.022.080, 5.136.646 en 5.204.691. Tevens, is het gebruik van elektronische gegevens of documentuitwisseling of EDI om zakencommunicaties van compagnon naar compagnon te verzenden bekend in de stand der techniek, zoals, bij wijze van voorbeeld, beschreven in het Amerikaanse octrooischrift 5.202.977 in het bezit van de hierin genoemde rechtverkrijgende, of in het eerder genoemde Amerikaanse octrooischrift 5.337.360. Echter zijn de aanvragers niet op de hoogte van succesvolle stand der techniek pogingen om het INTERNET, of een willekeurig ander ruim toegankelijk open netwerk, zoals telefoonlijnen of elk willekeurig TCP/IP systeem, te gebruiken waarin een veilig publieke sleutel/privé sleutel systeem, zoals RSA, succesvol gecombineerd is met EDI om authenticatie en niet-afwijzing van zowel oorsprong als ontvangst in een veilig compagnon-naar compagnon privé transactie te verschaffen die op een willekeurig tijdstip over het open netwerk kan optreden zonder wachtwoordbeheer te vereisen, terwijl tevens verificatie van berichtintegriteit verschaffend. Een dergelijk systeem elimineert de behoefte aan privé kleptoegevoegde netwerken en andere derde partij-privé netwerken alsmede het garanderen van de commerciële haalbaarheid van een privé compagnon-naar compagnon zakentransactie over een ruim toegankelijk open netwerk onder gebruikmaking van

EDI. De zekerheid van niet-afwijzing en authenticatie elimineert de mogelijkheid van elke partij om te ontkennen dat de transactie goed gekeurd was en elimineert twijfel met betrekking tot de inhoud van het EDI document dat aanleiding geeft tot de transactie. De mogelijkheid van de werkwijze en systeem van de onderhavige uitvinding om een veilig EDI bericht te verschaffen in combinatie met een RSA type publieke/privé sleutelsysteem verhelpt de nadelen van de stand der techniek.

Samenvatting van de uitvinding

De werkwijze en systeem van de onderhavige uitvinding omvat het gebruik van het AUTACK of EDI bevestigingsbericht als een document om de digitale ondertekening in een publieke/privé sleutelsysteem te verschaffen waarin het AUTACK ondertekend wordt door een gecodeerde hash code van de EDI uitwisselingscommunicatie die gecodeerd is met de privé sleutel van de zender, zoals in een RSA type publieke/privé sleutelsysteem, en is een verbetering van bekende systemen. Daar de AUTACK of functionele bevestiging verzekerd is met de privé sleutel van de zender van de functionele bevestiging, is de ontvanger van het oorspronkelijke bericht, wanneer de oorspronkelijke zender het antwoord AUTACK bericht decodeert met de publieke sleutel van de ontvanger, verzekerd dat de beoogde ontvanger werkelijk het antwoord AUTACK of bevestiging verzonden heeft en van de integriteit van de ontvangst vanwege de gedetecteerde correcte hash code.

Het EDI AUTACK bericht, zoals het EDIFACT AUTACK bericht, een generieke internationale standaard voor EDI voor administratie, handel en commercie, wordt bij voorkeur gebruikt om de gewenste veilige authenticatie, niet-afwijzing van oorsprong of ontvangst, en bevestiging of ontkenning van bevestiging voor één of meerdere EDI omhullingen, zoals bijvoorbeeld het X.12 of EDIFACT omhullingen te leveren. In de thans bevoorkeurde werkwijze en systeem van de onderhavige uitvinding, berekend in het proces van

authenticatie en niet-afwijzing van oorsprong, de zender een gewenste hash of berichtsamenvatting van de EDI, zoals de MD5 voor de gehele EDI uitwisselingscommunicatie, en voegt de waarde in in het AUTACK bericht. De zender berekent dan bij voorkeur de MD5 (berichtsamenvatting versie 5) van het AUTACK bericht en ondertekent digitaal het AUTACK door het coderen van de berekende MD5 met de privé sleutel van de zender, en voegt deze waarde in in het AUTACK bericht. Aldus wordt bij voorkeur het AUTACK, of EDI bevestigingsbericht gebruikt om de ondertekening te verschaffen. Na ontvangst van het bericht decodeert de ontvanger vervolgens de EDI uitwisselingscommunicatie, indien deze gecodeerd is, en berekent de MD5 van de ontvangen EDI uitwisselingscommunicatie. Indien niet-afwijzing van oorsprong gewenst is, decodeert de ontvanger vervolgens het AUTACK bericht met de publieke sleutel van de zender. De in dit voorbeeld door deze decodering verkregen waarde is de MD5 van het AUTACK bericht. De MD5 van het AUTACK bericht wordt vervolgens berekend en vergeleken met de gedecodeerde waarde. Indien beide waarden gelijk zijn, is de integriteit van het AUTACK geverifieerd en is niet-afwijzing van oorsprong tot stand gebracht. De MD5 van de EDI uitwisselingscommunicatie wordt vervolgens vergeleken met de MD5 van de EDI uitwisseling die ingevoerd is in het AUTACK en indien de twee gelijk zijn, wordt vervolgens de integriteit van de EDI uitwisseling geverifieerd, en wordt niet-afwijzing van oorsprong tot stand gebracht.

Teneinde vervolgens niet-afwijzing van ontvangst tot stand te brengen, na verificatie van de integriteit en authenticiteit van de op de bovenbeschreven manier ontvangen EDI uitwisselingscommunicatie, wordt een nieuwe of antwoord AUTACK opgewekt door het bezetten van alle segmenten en elementen, zoals geschikt, de berekende MD5 wordt digitaal ondertekend met de privé sleutel van de ontvanger, de digitaal ondertekende MD5 wordt ingevoegd in het antwoord AUTACK, geschikte segmenten van het antwoord AUTACK worden bezet, en het voorbereidde antwoord AUTACK wordt

verzonden naar de zender. De originele zender verifieert vervolgens na ontvangst van dit antwoord AUTACK, de digitale ondertekening van de ontvanger van zijn oorspronkelijk bericht door het doceren daarvan met de publieke sleutel van de ontvanger. De door deze decodering verkregen waarde is de MD5 van het ontvangen antwoord AUTACK. De oorspronkelijke zender, die het antwoord AUTACK van de ontvanger van zijn bericht heeft ontvangen, berekent vervolgens de MD5 van het ontvangen antwoord AUTACK en indien de berekende MD5 gelijk is aan de gedecodeerde MD5, is de integriteit van het AUTACK behouden en is niet-afwijzing van oorsprong van het AUTACK tot stand gebracht. Bovendien, indien de MD5 bevat in het bepaalde segment van het ontvangen AUTACK waar het door de zender ingevoerd is gelijk is aan de MD5 van de eerder verzonden EDI uitwisseling en de bevestiging positief is, hetgeen geconcludeerd kan worden door het testen van de veiligheidscode in het AUTACK bericht, dan is het volgende impliciet voor het tot stand brengen van het niet-afwijzing van ontvangst: de EDI uitwisselingscommunicatie in kwestie is bekend bij zowel zender als ontvanger daar de MD5 van de EDI uitwisselingscommunicatie en het uitwisselingsgetal bevat zijn in het AUTACK bericht en naar behoren herkend zijn, is de integriteit en authenticiteit van de EDI uitwisselingscommunicatie bij ontvangst geverifieerd, en ontkent de ontvanger niet de betreffende EDI uitwisselingscommunicatie ontvangen te hebben.

De mogelijkheid om te handelen of zaken te doen op een compagnon-tot-compagnonbasis over een open publiek netwerk, zoals het INTERNET, zonder de noodzaak voor wachtwoordbeheer kan geregeld worden, tot de gewenste mate, door de handelsdeelnemers door het gebruik van handelspartnerovereenkomsten (TPA) om sleuteluitwisselingcertificatie te verschaffen, of door het vertrouwen op een certificaat autoriteit die publieke/privé sleutelwegen uitgeeft en verifieert. Aldus, kunnen privé en veilige transacties, onderworpen aan authenticatie en niet-afwijzing van zowel oorsprong als ontvangst, samen met verificatie van bericht

integriteit, onder gebruikmaking van EDI, over een open communicatie netwerk uitgevoerd worden.

KORTE BESCHRIJVING VAN DE TEKENINGEN

Figuur 1 is een functioneel stroomdiagram van de thans bevoorkeurde werkwijze en systeem van de onderhavige uitvinding voor het verschaffen van veilige EDI over een open netwerk, zoals het INTERNET, teneinde integriteit, authenticatie, niet-afwijzing van oorsprong en ontvangst, en vertrouwelijkheid te verschaffen onder gebruikmaking van EDI;

Figuur 2 is een functioneel stroomdiagram van het deel van de werkwijze en systeem van figuur 1 dat authenticatie en niet-afwijzing van oorsprong verschaft onder gebruikmaking van het EDIFACT AUTACK bericht;

Figuur 3 is een functioneel stroomdiagram, analoog aan figuur 2, van het deel van de werkwijze en systeem van figuur 1 dat niet-afwijzing van ontvangst verschaft onder gebruikmaking van het EDIFACT AUTACK bericht;

Figuur 4 is een functioneel stroomdiagram van de ontvangst van veilige post over het INTERNET in overeenkomst met de thans bevoorkeurde werkwijze en systeem van de onderhavige uitvinding;

Figuur 5 is een functioneel stroomdiagram, analoog aan figuur 4, voor het zenden van veilige post over het INTERNET in overeenstemming met de thans bevoorkeurde werkwijze en systeem van de onderhavige uitvinding;

Figuur 6 is een functioneel stroomdiagram, analoog aan figuur 4, van handelspartnerbeheer in overeenkomst met de thans bevoorkeurde werkwijze en systeem van de onderhavige uitvinding;

Figuur 7 is een functioneel stroomdiagram, analoog aan figuur 4, van auditlog beheer in overeenstemming met de thans bevoorkeurde werkwijze en systeem van de onderhavige uitvinding;

Figuur 8 is een functioneel stroomdiagram, analoog aan figuur 4, van volgbeheer in overeenstemming met de

thans bevoorkeurde werkwijze en systeem van de onderhavige uitvinding;

Figuur 9 is een functioneel stroomdiagram, analoog aan figuur 4, van bewerkingsbewaking in overeenstemming met de thans bevoorkeurde werkwijze en systeem van de onderhavige uitvinding;

Figuur 10 is een functioneel diagram, van de organisatie van het systeem gebruikt in het uitvoeren van de thans bevoorkeurde werkwijze van de onderhavige uitvinding;

Figuren 11-13 bevatten een functioneel stroomdiagram, analoog aan figuur 4, van de algehele thans bevoorkeurde werkwijze en systeem van figuren 1-10, waarbij figuur 11 certificaatverificatie toont, figuur 12 TPA (=handelspartnerovereenkomst) verwerking toont, en figuur 13 publieke sleutel/privé sleutel verwerking toont;

Figuur 14 is een diagrammatische illustratie van een typisch computerschermdisplay in overeenstemming met de thans bevoorkeurde werkwijze en systeem van de onderhavige uitvinding, tonen de verscheidene functionele opties die gestuurd dienen te worden door de gebruikers om veilige post over het INTERNET te garanderen in overeenstemming met de thans bevoorkeurde werkwijze en systeem van de onderhavige uitvinding.

Figuren 15-21 zijn diagrammatische illustraties, analoog aan figuur 14, van typische computerschermdisplays in overeenstemming met de HANDELSPARTNERS PROFIEL optie in het schermdisplay van figuur 14;

Figuren 22-28 zijn diagrammatische illustraties, analoog aan figuur 14, van typische computerschermdisplays in overeenstemming met de HANDELSPARTNEROVEREENKOMSTEN (TPA) optie in het schermdisplay van figuur 14, waarbij figuur 18 het UITGAAND HERVERZENDING schermdisplay voor het verzenden van veilige E-post in overeenstemming met de thans bevoorkeurde werkwijze en systeem van de onderhavige uitvinding toont;

Figuren 29-33 zijn diagrammatische illustraties, analoog aan figuur 14, van typische computerschermdisplays in overeenstemming met de SLEUTELBEHEER optie in het schermdisplay van figuur 14; en

Figuren 34-41 zijn diagrammatische illustraties, analoog aan figuur 14, waarvan typische computerschermdisplays in overeenstemming met de VOLG optie in het schermdisplay van figuur 14, waarbij figuren 35-38 het volgen van uitwisselingen en figuren 39-41 het volgen van een audit log tonen.

Gedetailleerde beschrijving van de bevoorkeurde uitvoeringsvorm

Verwijzende nu naar de tekeningen in detail, en initieel naar figuur 1, wordt een functioneel stroomdiagram van het thans bevoorkeurde systeem 100 van de onderhavige uitvinding voor het verschaffen van veilige EDI over een conventioneel open netwerk, zoals het commercieel verkrijgbare INTERNET 102, getoond. De bevoorkeurde werkwijze en systeem van de onderhavige uitvinding is geïmplementeerd in een systeem dat verschaft wordt onder het handelsmerk TEMPLAR in het bezit van de hierin genoemde rechtverkrijgende. Zoals in groter detail hierna zal worden uitgelegd, met verwijzing naar figuren 2-41, verschaft de thans bevoorkeurde werkwijze en systeem van de onderhavige uitvinding integriteit, authenticatie, niet-afwijzing van zowel oorsprong als ontvangst, en vertrouwelijkheid onder gebruikmaking van EDI. Dit wordt bij voorkeur bereikt door gebruik te maken van het AUTACK of EDI (Electronic Data Interchange, elektronische gegevensuitwisseling) bevestigingsbericht als een document om digitale ondertekening in een publieke/privésleutelsysteem te verschaffen, dat er bij voorkeur één is dat gebruik maakt van het conventionele RSA publieke/privésleutelcoderingsschema, zoals het coderingsschema beschreven in de Amerikaanse octrooischriften 4.405.828; 4.424.414; 4.200.770, en 4.218.582, de inhoud waarvan hierin in zijn volledigheid door verwijzing is

opgenomen. Zoals hierna in grotere detail beschreven zal worden, wordt het AUTACK bij voorkeur verzegeld of ondertekend met een digitale ondertekening die bij voorkeur opgewekt wordt door het coderen van de MD5 (message digest version 5, bericht samenvatting versie 5) van het AUTACK met voortbrenger van de privésleutel van het AUTACK, zoals de privésleutel van de zender in het bevoorkeurde proces van authenticatie en niet-afwijzing van oorsprong getoond in figuur 2, of met de privésleutel van de ontvanger in het bevoorkeurde proces van niet-afwijzing van ontvangst getoond in figuur 3. De digitale ondertekening wordt vervolgens bij voorkeur ingevoerd in een voorafbepaalde positie in het AUTACK en verzonden naar de andere partij in de transactie. Daar het AUTACK verzegeld is met de privésleutel van de zender van de AUTACK, wanneer de ontvanger van dit AUTACK het AUTACK decodeert met de publieke sleutel van de zender van dit AUTACK, is hij verzekerd dat de beoogde ontvanger van zijn bericht werkelijk dit AUTACK verzonden heeft, alsmede verzekerd van de integriteit van de ontvangst vanwege de, op de manier zoals hierna beschreven zal worden, detectie van de correcte hash code. In overeenstemming met de onderhavige uitvinding, zijn de gecodeerde geheime sleutel gebruikt om het bericht te coderen, alsmede het bericht zelf, in het PKCS bericht opgenomen.

De MD5 is een conventionele waarde die verkregen kan worden in een EDI bericht door het conventioneel hashen van een kwantiteit, zoals een EDI uitwisseling. Er is een zeer lage waarschijnlijkheid dat de MD5 van willekeurig twee verschillende documenten identiek zal zijn, en dienovereenkomstig, wordt de MD5 bij voorkeur gebruikt om de integriteit van EDI uitwisselingen in overeenstemming met de thans bevoorkeurde werkwijze van de onderhavige uitvinding tot stand te brengen.

Zoals bekend is bij gebruikers van EDI, is een AUTACK bericht een UN/EDIFACT standaard voor authenticatie en bevestiging. In overeenstemming met de thans bevoorkeurde werkwijze en systeem van de onderhavige uitvinding,

bestaat het AUTACK bij voorkeur uit de USH of veiligheidskop, USB, USX om het bericht te identificeren, USY om de veiligheidsinformatie op het betroffen bericht te houden, USR, en een paar andere conventionele segmenten die normaal in een AUTACK gevonden worden. Bij voorkeur, worden informatie zoals reactietype, omvang van veiligheidstoepassing, en veiligheidsfunctie in het USH segment gecodeerd. Bij wijze van voorbeeld, kan het tweede element van het USH segment bij voorkeur de waarde 2 bevatten, of een bepaalde andere aangewezen waarde, indien het AUTACK zou dienen als een document verifiërende niet-afwijzing van oorsprong met, bijvoorbeeld, het vijfde veld hebbende de waarde 2, of een bepaalde andere aangewezen waarde, indien een bevestiging vereist zou zijn. Het USX segment bevat bij voorkeur het uitwisselingsgetal van de EDI uitwisseling in kwestie, daardoor het betreffende bericht verbindende met het AUTACK, en het USR segment is bij voorkeur een veiligheidsresultaatvasthouder en bevat de digitaal ondertekende MD5 van het AUTACK in overeenstemming met de onderhavige uitvinding.

Zoals verder getoond en bevoorkeurd in figuur 1, uitsluitend een twee partijen zakentransactie tussen twee partijen aannemend die een handelspartnerovereenkomst aangegaan zijn, waarbij elk van de partijen een conventioneel computerwerkstation 104, 106 heeft, zoals een RS/6000, HP/9000 en SOLARIS; een conventionele EDI vertaler 108, 110; een conventionele geïntegreerde software/hardware server 112, 114, die geprogrammeerd is om te werken in overeenstemming met de bevoorkeurde werkwijze en systeem van de onderhavige uitvinding, en die conventionele computerdisplayterminals 116, 118 bevat, in staat tot het werken in een microsoft WINDOWS of UNIX X-WINDOWS type omgeving, voor het weergeven van berichten en keuzes in overeenstemming met de bevoorkeurde werkwijze van de onderhavige uitvinding alsmede berichten en documenten verzonden via EDI over het INTERNET netwerk 102 bij het uitvoeren van de werkwijze van de onderhavige uitvinding, waarbij de servers

112, 114 in staat zijn tot het verschaffen van de gewenste authenticatie, integriteit, niet-afwijzing van oorsprong en ontvangst, en vertrouwelijkheid in overeenstemming met de onderhavige uitvinding. Zoals getoond en bevoorkeurd, communiceren de servers 112, 114 conventioneel over het open netwerk, zoals het INTERNET 102, door een heterogene postomgeving 120, 122, zoals eentje die gebruik maakt van SMPT/MIME, X400/X435, LOTUS NOTES/cc:MAIL, en/of MICROSOFT MAIL/EXCHANGE. De servers, 112, 114 zijn bij voorkeur conventionele computers, die conventioneel geprogrammeerd zijn in C++, om de thans bevoorkeurde werkwijze van de onderhavige uitvinding uit te voeren, en zijn bij voorkeur gericht op het lopen op één van de volgende UNIX platforms: AIX, HPUX, SUN OS, of SOLARIS.

Beneden in tabel A zijn de verscheidene manuscripten opgesomd die eenvoudig door een programmeur van normale kundigheid in het gebied gebruikt kunnen worden om de noodzakelijke programmering in C++ op te wekken, die een object georiënteerde programmeertaal is, om te lopen op de servers 112, 114 om de thans bevoorkeurde werkwijze van de onderhavige uitvinding uit te voeren. Zoals opgemerkt zal worden, hebben de verscheidene manuscripts betrekking op het verzenden van een EDI document, het herverzenden van een EDI document, het ontvangen van een veilig EDI document, het ontvangen van een bevestigings AUTACK, het ontvangen van een nieuwe publieke sleutel van een handelspartner, het verdelen van jouw nieuwe publieke sleutel onder gerelateerde handelspartners, het activeren van het certificaatbeheer hoofdmenu, het opwekken van je eigen privé/publieke sleutelpaar, het veranderen van een certificaat (je eigen publieke/privé sleutelpaar), het verwijderen van je eigen privé/publieke sleutelpaar, het kopiëren van je eigen publieke sleutel naar het diskbestand, het afdrukken van je eigen publieke sleutelcertificaat, het opslaan van je eigen privé/publieke sleutel in de diskfile, het heropslaan van je eigen privé/publieke sleutel van je diskbestand om de bestaande privé/publieke sleutel te

vervangen, het heropslaan van je eigen privé/publieke sleutel van de diskfile naar een nieuwe sleutel, het activeren van het handelspartner publieke sleutelbeheer hoofdmenu, het toevoegen van een handelspartner publieke sleutel, het veranderen van de handelspartner publieke sleutel, het verwijderen van de handelspartner publieke sleutel, het kopiëren van de handelspartner publieke sleutel van het diskbestand om de bestaande handelspartner publieke sleutel te vervangen, het kopiëren van de handelspartner publieke sleutel van de diskfile naar een nieuwe sleutel, het activeren van het handelspartnerovereenkomst beheerhoofdmenu, het toevoegen van handelspartnerovereenkomst, het veranderen van de handelspartnerovereenkomst, het verwijderen van de handelspartnerovereenkomst, het kopiëren van de handelspartnerovereenkomst naar het diskbestand, het kopiëren van de handelspartnerovereenkomst van het diskbestand, MIME pakkettering (conventioneel MIME bericht), MIME ontpakkettering, PKCS pakkettering (conventioneel PKCS), PKCS ontpakkettering, het werken met volgbestand, het bewaken van serverbewerkingen, het ontvangen van een ongeldig EDI document met een integriteitsprobleem, het ontvangen van een AUTACK met een integriteitsprobleem, het ontvangen van niet ondersteunde post, het ontvangen van een EDI uitwisseling zonder AUTACK terwijl niet-afwijzing van oorsprong verwacht is, en het ontvangen van een onverwacht AUTACK.

Tabel A

MANUSCRIPTEN

Het verzenden van een EDI document

Initiator	Actie	Deelnemer
EDI vertaler	Verzoek om een EDI groep te verzenden	Authenticatie agent
Authenticatie-agent	Verkrijg zender en ontvanger ID	EDI uitwisselingsomhulling
Authenticatie-agent	Creëer een volgbestand	Volgbestand
Authenticatie-agent	Creëer een gebeurtenis beginlogingave	Audit log
Authenticatie-agent	Verzoek samenvattingsberekeningswerkwijze en bestemmingsadres van handelspartner, bronadres, werkwijze van niet-afwijzing van ontvangst (NRR), niet-afwijzing van oorsprong (NRO), vertrouwelijkheid en overdracht	Handelspartnerovereenkomst
Authenticatie-agent	Verkrijg identificatiesamenvatting	EDI uitwisseling
EDI uitwisseling	Verkrijg identificatiesamenvattingswerk-wijze	Configuratie
EDI uitwisseling	Bereken samenvatting van de EDI uitwisse-ling	Calculatorsamenvatting
Authenticatie-agent	Verifieer of de stuurgetal en de identi-ficatiesamenvatting uniek is	Volglijst
Authenticatie-agent	Creëer AUTACK	AUTACK
AUTACK	Verkrijg de privésleutel ID, NRR, NRO, integriteitscontrole, samenvattingswerk-wijze	Handelspartnerovereenkomst
AUTACK	Verkrijg de privésleutel	Sleutelindex
AUTACK	Verkrijg integriteits-samenvatting	EDI uitwisseling
AUTACK	Bereken eigen samenvatting	Calculatorsamenvatting
AUTACK	Onderteken de samenvatting van het AUTACK	BSAFE
Authenticatie-agent	Creëer AUTACK omhulling	UNB omhulling
Authenticatie-agent	Codeer de EDI uitwisseling	PKCS
Authenticatie-agent	Combineer de EDI uitwisseling en AUTACK in één MIME gecodeerd postlichaam (meer-voudige MIME delen)	MIME pakkettering
Authenticatie-agent	Verzend de gecodeerde uitwisseling naar handelspartner	Verzend post
Authenticatie-agent	Werk het volgbestand bij met de zenddatum en tijd, lokatie van het zendlichaam, zender en ontvanger ID, NRO en integri-teitssamenvatting, privé-sleutel ID, pu-blieke sleutel ID, identificatiesamenvat-ting	Volgbestand
Authenticatie-agent	Creëer een verzonden post logingang	Audit log
Authenticatie-agent	Retourneer een succes retourcode en volg-bestand ID naar EDI vertaler	Authenticatie-agent

Herverzending van een EDI document

Initiator	Actie	Deelnemer
Herverzend monitor	Verzoek de bevestigingsstatus	Volgbestand
Herverzend monitor	Verzoek herverzendactie	Handelspartnerovereenkomst
Herverzend monitor	Verzoek om herverzending van de EDI uitwisseling	Authenticatie-agent
Authenticatie-agent	Verzoek de lokatie van het postlichaam	Volgbestand
Authenticatie-agent	Verzend de gecodeerde uitwisseling naar handelspartner	Verzend post
Authenticatie-agent	Werk het volgbestand bij met herverzenddatum en tijd	Volgbestand
Authenticatie-agent	Creëer een her-verzonden post log ingang	Audit log

Ontvang een geldig EDI document

Initiator	Actie	Deelnemer
MIME pakkettering	Informeer postaankomst	MIME pakkettering
Authenticatie-agent	Creëer een succesvol ontvangen post log ingang	Audit log
Authenticatie-agent	Valideer dat de ontvangen post een EDI uitwisseling bevatte	EDI uitwisseling
Authenticatie-agent	Creëer een volgbestand	Volgbestand
Authenticatie-agent	Verkrijg zender en ontvanger ID	EDI uitwisselingsomhuling
Authenticatie-agent	Verkrijg handelspartner overeenkomst met zender en ontvanger ID	Handelspartnerovereenkomst
Authenticatie-agent	Verkrijg de samenvatting van de uitwisseling en ondertekende samenvatting, en samenvatting berekeningswerkwijze	AUTACK
AUTACK	Verkrijg de publieke sleutel ID	Handelspartnerovereenkomst
AUTACK	Verkrijg de publieke sleutel van de handelspartner	Sleutelindex
Sleutelindex	Lees de laatst effectieve publieke sleutel	Sleutelindex
AUTACK	Decodeer de ondertekende samenvatting	BSAFE
Authenticatie-agent	Bereken samenvatting van de EDI uitwisseling	EDI uitwisseling
Authenticatie-agent	Vergelijk de berekende samenvatting van de EDI uitwisseling met de samenvatting in het AUTACK; verifieer dat de samenvatting van het deel AUTACK hetzelfde is als de gedecodeerde ondertekende samenvatting in het AUTACK	AUTACK
Authenticatie-agent	Verkrijg identificatie samenvatting	EDI uitwisseling
EDI uitwisseling	Verkrijg identificatie samenvattingwerkwijze	Configuratie
EDI uitwisseling	Samenvatting van de EDI uitwisseling	Calculator samenvatting

Initiator	Actie	Deelnemer
Authenticatie-agent	Verifieer dat de stuurgetal en identificatiesamenvatting uniek is	Volglijst
Authenticatie-agent	Creëer een succesvol ontvangen EDI uitwisselingslogingang	Audit log
Authenticatie-agent	Verkrijg de niet-afwijzing van ontvangstvlag	Handelspartnerovereenkomst
Authenticatie-agent	Creëer een bevestigings AUTACK stuurgetal	AUTACK
AUTACK	Verkrijg de privésleutel ID	Handelspartnerovereenkomst
AUTACK	Verkrijg de privésleutel	Sleutelindex
AUTACK	Onderteken de samenvatting	BSAFE
Authenticatie-agent	Creëer een AUTACK verzendverzoeklogingang	Audit log
Authenticatie-agent	Creëer een AUTACK MIME gecodeerd postlichaam	MIME pakkettering
Authenticatie-agent	Verzend het gecodeerde AUTACK naar handelspartner	Verzend post
Authenticatie-agent	Werk het volgbestand bij met AUTACK verzenddatum en tijd, plaats van het postlichaam, zender en ontvanger ID, samenvatting	Volgbestand
Authenticatie-agent	Creëer een verzonden AUTACK logingang	Audit log
Authenticatie-agent	Verkrijg ingaande routeringspost-verwerkingsactie	Handelspartnerovereenkomst
Authenticatie-agent	Schrijf EDI gegevens naar gespecificeerd bestand of index	Authenticatie-agent
Authenticatie-agent	Voer post-verwerkingscommando uit (bijvoorbeeld roep EDI vertaler aan)	Authenticatie-agent

Ontvang een bevestigings AUTACK

Initiator	Actie	Deelnemer
MIME pakkettering	Informeer postaankomst	MIME pakkettering
Authenticatie-agent	Verkrijg lijst van MIME lichaamsdelen	MIME pakkettering
Authenticatie-agent	Valideer dat ontvangen post een AUTACK bevatte	AUTACK uitwisseling
Authenticatie-agent	Verkrijg zender en ontvanger ID	AUTACK uitwisselingsomhulling
Authenticatie-agent	Verkrijg NRR vlag, publieke sleutel ID	Handelspartnerovereenkomst
Authenticatie-agent	Verifieer de ondertekening van de zender	BSAFE
Authenticatie-agent	Verkrijg uitwisselings stuurgetal en integriteitssamenvatting	AUTACK
Authenticatie-agent	Werk bevestiging ontvangen datum en tijd van de verzonden uitwisseling bij	Volgbestand

Ontvang een nieuwe publieke sleutel van een handelspartner

Initiator	Actie	Deelnemer
MIME pakkettering	Informeer postaankomst	MIME pakkettering
Authenticatie-agent	Verkrijg lijst van MIME lichaamsdelen	MIME pakkettering
Authenticatie-agent	Valideer dat de ontvangen post een certificaat bevatte	Certificaat
Authenticatie-agent	Verkrijg onderscheidend naam, kwalificerend element en ID van de handelspartner	Cerficitaat
Authenticatie-agent	Verkrijg E-postadres van certificaatmanagementstaf, publieke sleutel	Sleutelindex
Authenticatie-agent	Verifieer de ondertekening	BSAFE
Authenticatie-agent	Log certificaataankomst	Audit log
Authenticatie-agent	Creëer een volgbestand met type certificaat	Volgbestand
Authenticatie-agent	Informeer de gebruiker van de aankomst van het certificaat	Authenticatie-agent
Gebruiker	Verifieer met handelspartner dat het certificaat correct is	Gebruiker
Gebruiker	Selecteer om het certificaat bij te werken van het volgbestand	Gebruiker
UI	Verkrijg het certificaat	Volgbestand
UI	Voeg aan het certificaat een nieuw serienummer toe	Sleutelindex
UI	Verander de verlopen datum van eerder certificaat	Sleutelindex
UI	Log certificaat bijwerking	Audit log
UI	Verander de status van het volgbestand dat bijgewerkt dient te worden	Volgbestand

Verdeel nieuwe eigen publieke sleutel onder gerelateerde handelspartners

Initiator	Actie	Deelnemer
Gebruiker	Aanspreken van certificaatbeheerknop	Gebruiker
UI	Verkrijg een lijst van sleutelpaar - sleutel ID	Sleutelindex
UI	Geef de lijst van sleutelpaar op scherm weer	UI
Gebruiker	Selecteer het certificaat om te distribueren	Gebruiker
Gebruiker	Roep de distributiefunctie op	Gebruiker
UI	Verkrijg een lijst van handelspartner die gebruik maakt van dat certificaat	Handelspartnerovereenkomst
UI	Verkrijg het E-postadres van de handelspartner	Handelspartner
UI	Geef de lijst van handelspartner en E-postadres weer	UI
Gebruiker	Selecteer of deselecteer handelspartner	Gebruiker

Initiator	Actie	Deelnemer
Gebruiker	Verander het E-postadres	Gebruiker
Gebruiker	Voeg een nieuw E-postadres toe	Gebruiker
Gebruiker	Roep het distributieproces op	Gebruiker
UI	Creëer het certificaat (X.509 of PKCS?)	Sleutelindex
UI	Codeer het certificaat in MIME formaat	MIME pakkettering
UI	Verzend het MIME gecodeerde certificaat	Verzend post
UI	Creëer een verzonden sleutel logingang	Audit log

Activeer certificaatbeheer hoofdmenu

Initiator	Actie	Deelnemer
Gebruiker	Aanspreken van certificaatbeheerknop	Gebruiker
UI	Verkrijg een lijst van sleutelpaar - sleutel ID	Sleutelindex
UI	Geef de lijst van sleutelpaar op scherm weer	UI

Creëer eigen privé/publieke sleutelpaar

De gebruiker dient in te loggen en het certificaatbeheer-hoofdmenu te activeren alvorens tot deze functie te komen.

Initiator	Actie	Deelnemer
Gebruiker	Aanspreken van creëer sleutelpaarknop	Gebruiker
UI	Geef een scherm weer om sleutel ID, effectieve datum, onderscheiden naam en E-postadres te accepteren	UI
Gebruiker	Toets de sleutel ID, effectieve datum, naam en E-postadres in	Gebruiker
UI	Creëer sleutelpaar	Sleutelindex
Sleutelindex	Verkrijg lengte van de sleutel	Configuratie
Sleutelindex	Verkrijg sleutel opwekkingszaad	Zaadgenerator
Sleutelindex	Wek privé en publieke sleutelpaar op	BSAFE
Sleutelindex	Nagaan of de publieke sleutel niet bestaat	Sleutelindex database
Sleutelindex	Verkrijg interne coderingssleutel	Configuratie
Sleutelindex	Codeer de privésleutel	BSAFE
Sleutelindex	Wijs 1 toe aan het serienummer	Sleutelindex
Sleutelindex	Schrijf het sleutelpaar	Database
Sleutelindex	Retourneer het sleutelpaar	Sleutelindex
UI	Werk sleutellijst bij	UI

Verander certificaat (eigen privé/publieke sleutelpaar)

De gebruiker dient in te loggen en het certificaatbeheer hoofdmenu te activeren alvorens tot deze functie te komen.

Initiator	Actie	Deelnemer
Gebruiker	Selecteer een sleutelpaar voor verandering	Gebruiker
Gebruiker	Spreek veranderingscertificaatknop aan	Gebruiker
UI	Geef een scherm weer om effectieve datum, naam en E-postadres te veranderen	Gebruiker
Gebruiker	Verander velden	Gebruiker
Gebruiker	Spreek de creëer nieuwe sleutelknop aan	Gebruiker
UI	Heropwekken van het sleutelpaar	Sleutelindex
Sleutelindex	Wijs een nieuw serienummer toe	Sleutelindex
Sleutelindex	Verkrijg sleutel opwekkingszaad	Zaadgenerator
Sleutelindex	Verkrijg lengte van de sleutel	Configuratie
Sleutelindex	Wek privé en publieke sleutelpaar op	BSAFE
Sleutelindex	Nagaan of de publieke sleutel niet bestaat	Sleutelindex database
Sleutelindex	Verkrijg interne coderingssleutel	configuratie
Sleutelindex	Codeer de privésleutel	BSAFE
Sleutelindex	Schrijf het nieuwe sleutelpaar	Sleutelindex-database
Sleutelindex	Retourneer het sleutelpaar	Sleutelindex
UI	Werk sleutellijst bij	UI

Verwijder eigen privé/publieke sleutelpaar

De gebruiker dient in te loggen en het certificaatbeheer hoofdmenu te activeren alvorens tot deze functie te komen.

Initiator	Actie	Deelnemer
Gebruiker	Selecteer een sleutelpaar voor verwijdering	Gebruiker
Gebruiker	Spreek verwijder sleutel-paarknop aan	Gebruiker
UI	Controleer of het sleutelpaar gebruikt is in een handelspartnerovereenkomst	Handelspartnerovereenkomst
UI	Geef het bevestigingsbericht weer	UI
Gebruiker	Bevestig het verwijderen van het sleutelpaar	Gebruiker
UI	Verwijder het sleutelpaar	Sleutelindex
Sleutelindex	Deactiveer het sleutelpaar	Sleutelindex database
UI	Markeer het sleutelpaar als gedeactiveerd op scherm	UI

Kopieer eigen publieke sleutel naar diskbestand

De gebruiker dient in te loggen en het certificaatbeheer hoofdmenu te activeren alvorens tot deze functie te komen.

Initiator	Actie	Deelnemer
Gebruiker	Selecteer een sleutel	Gebruiker
Gebruiker	Roep de kopieer naar diskfunctie op	Gebruiker
UI	Geef een scherm weer om te vragen voor de uitvoer bestandsnaam	UI
Gebruiker	Toets de bestandsnaam in	Gebruiker
UI	Geef een vervangingsbevestigingsscherm weer	UI
Gebruiker	Selecteer om het bestaande bestand over te schrijven	Gebruiker
UI	Voer het certificaat in X.509 formaat uit naar diskbestand	Sleutelindex
UI	Geef een voltooiingsbericht weer	UI
UI	Geef de lijst opnieuw weer	UI

Druk eigen publieke sleutelcertificaat af

De gebruiker dient in te loggen en het certificaatbeheer hoofdmenu te activeren alvorens tot deze functie te komen.

Initiator	Actie	Deelnemer
Gebruiker	Selecteer een sleutel	Gebruiker
Gebruiker	Roep de afdrukcertificaatfunctie op	Gebruiker
UI	Verkrijg het door een mens leesbare geformatteerde certificaat	Sleutelindex
Sleutelindex	Formatteer de onderscheiden naam, publieke sleutel, effectieve datum, referentie (sleutel ID), serienummer, ondertekeningsalgoritme, certificaatondertekening, versie, afgever en E-postadres	Sleutelindex
UI	Voer het certificaat uit naar de systeem gekozen printer	UI
UI	Geef de lijst opnieuw weer	UI

Sla eigen privé/publieke sleutel op in diskbestand

De gebruiker dient in te loggen en het certificaatbeheer hoofdmenu te activeren alvorens tot deze functie te komen.

Initiator	Actie	Deelnemer
Gebruiker	Selecteer een sleutel	Gebruiker
Gebruiker	Roep de opslaan in diskfunctie op	Gebruiker
UI	Geef een scherm weer om te vragen voor de uitvoer bestandsnaam	UI
Gebruiker	Toets de bestandsnaam in	Gebruiker
UI	Geef een vervangingsbevestigingsscherm weer	UI
Gebruiker	Selecteer om het bestaande bestand over te schrijven	Gebruiker
UI	Voer het sleutelpaar, onderscheiden naam, privé, publieke sleutel, effectieve datum, referentie (sleutel ID), serienummer, samenvattingsalgoritme, samenvatting, versie, afgever en E-post-adres uit naar bestand	Sleutelindex
UI	Geef een voltooiingsbericht weer	UI
UI	Geef de lijst opnieuw weer	UI

Opnieuw opslaan van eigen privé/publieke sleutel van diskbestand om de bestaande te vervangen

De gebruiker dient in te loggen en het certificaatbeheer hoofdmenu te activeren alvorens tot deze functie te komen.

Initiator	Actie	Deelnemer
Gebruiker	Selecteer een sleutel	Gebruiker
Gebruiker	Roep de opnieuw opslaan van diskfunctie op	Gebruiker
UI	Geef een scherm weer om te vragen voor de invoer bestandsnaam	UI
Gebruiker	Toets de bestandsnaam in	Gebruiker
UI	Geef een vervangingsbevestigings en opslaan van het sleutel-paarscherm weer	UI
Gebruiker	Selecteer om de bestaande sleutel over te schrijven en toets de opslaan bestandsnaam in	Gebruiker
UI	Creëer een log ingang	audit log
UI	Voer het bestaande sleutelpaar, onderscheiden naam, privé, publieke sleutel, effectieve datum, referentie (sleutel ID), serienummer, samenvattingsalgoritme, samenvatting, versie, afgever en E-postadres uit naar het opslaan bestand	Sleutelindex
UI	Vervang het sleutelpaar	Sleutelindex
Sleutelindex	Lees de sleutelinformatie in van het bestand	Sleutelindex
Sleutelindex	Werk de sleutelinformatie bij	Database
UI	Geef een voltooiingsbericht weer	UI
UI	Geef de lijst opnieuw weer	UI

Opnieuw opslaan van eigen privé/publieke sleutel van diskbestand naar een nieuwe sleutel

De gebruiker dient in te loggen en het certificaatbeheer hoofdmenu te activeren alvorens tot deze functie te komen.

Initiator	Actie	Deelnemer
Gebruiker	Roep de opnieuw opslaan van diskfunctie op	Gebruiker
UI	Geef een scherm weer om te vragen voor de sleutel ID en invoer bestandsnaam	UI
Gebruiker	Toets de sleutel ID en bestandsnaam in	Gebruiker
Sleutelindex	Lees de sleutelinformatie in van het bestand	Sleutelindex
Sleutelindex	Bereken de certificaatsamenvatting	Samenvattingscalculator
Sleutelindex	Verifieer de samenvattingsovereenkomst	Sleutelindex
Sleutelindex	Schrijf de sleutelinformatie	databas
UI	Voeg het sleutelpaar toe aan de lijst	UI
UI	Geef de lijst opnieuw weer	UI

Activeer handelspartner publieke sleutel beheer hoofdmenu

Initiator	Actie	Deelnemer
Gebruiker	Spreek handelspartner sleutelknop aan	Gebruiker
UI	Verkrijg een lijst van handelspartner publieke sleutel	Sleutelindex
UI	Geef de lijst van handelspartner publieke sleutels op scherm weer	UI

Voeg handelspartner publieke sleutel toe

Gebruiker dient in te loggen en handelspartner publieke certificaatbeheer hoofdmenu te activeren alvorens tot deze functie te komen.

Initiator	Actie	Deelnemer
Gebruiker	Spreek de toevoegen handelspartner publieke sleutelknop aan	Gebruiker
UI	Geef toevoegen handelspartner publieke sleutelscherm weer	UI
Gebruiker	Selecteer om sleutel van een diskbestand toe te voegen	Gebruiker
UI	Geef een scherm weer voor het intoetsen van de bestandsnaam	UI
Gebruiker	Toets de bestandnaam in	Gebruiker
UI	Lees het E-postadres, effectieve datum, publieke sleutel, telefoonnummer, straatadres in	publieke sleutelbestand
UI	Geef de publieke sleutel weer	UI

Initiator	Actie	Deelnemer
Gebruiker	Toets de handelspartner firmanaam in	Gebruiker
UI	Geef de nieuwe publieke sleutel op de lijst op het scherm weer	UI

Verander handelspartner publieke sleutel

De gebruiker dient in te loggen en handelspartner publieke certificaatbeheer hoofdmenu te activeren alvorens tot deze functie te komen.

Initiator	Actie	Deelnemer
Gebruiker	Selecteer een publieke sleutel voor verandering	Gebruiker
Gebruiker	Spreek de verander publieke sleutelknop aan	Gebruiker
UI	Verkrijg de publieke sleutelinformatie	Sleutelindex
UI	Geef handelspartner publieke sleutel op scherm weer	UI
Gebruiker	Verander de effectieve datum en publieke sleutel	Gebruiker
UI	Werk de publieke sleutel bij	Sleutelindex
UI	Voeg aan de nieuwe publieke sleutel het serienummer toe	Sleutelindex
UI	Geef de nieuwe publieke sleutel in de lijst op scherm weer	UI

Verwijder handelspartner publieke sleutel

De gebruiker dient in te loggen en handelspartner publieke certificaatbeheer hoofdmenu te activeren alvorens tot deze functie te komen.

Initiator	Actie	Deelnemer
Gebruiker	Selecteer een publieke sleutel voor verwijdering	Gebruiker
Gebruiker	Spreek de verwijder publieke sleutelknop aan	Gebruiker
UI	Verkrijg de publieke sleutelinformatie	Sleutelindex
UI	Geef toevoegen handelspartner publieke sleutelscherm weer	UI
UI	Geef het bevestigingsscherm weer	UI
Gebruiker	Bevestig de verwijdering	Gebruiker
UI	Deactiveer de publieke sleutel	Sleutelindex
UI	Verwijder de publieke sleutel van de lijst op scherm	UI

Kopieer handelspartner publieke sleutel van diskbestand om de bestaande te vervangen

De gebruiker dient in te loggen en het certificaatbeheer hoofdmenu te activeren alvorens tot deze functie te komen.

Neem aan dat het bestand in X.509 formaat is.

Initiator	Actie	Deelnemer
Gebruiker	Selecteer een publieke sleutel	Gebruiker
Gebruiker	Roep de opnieuw opslaan van diskfunctie op	Gebruiker
UI	Geef een scherm weer om te vragen voor de invoer bestandsnaam	UI
Gebruiker	Toets de bestandsnaam in	Gebruiker
UI	Geef een vervangingsbevestiging en opslaan van het sleutelpaar-scherm weer	UI
Gebruiker	Selecteer om de bestaande sleutel over te schrijven en toets de opslaan bestandsnaam in	Gebruiker
UI	Creëer een log ingang	Auditlog
UI	Voer de bestaande sleutel-onderscheiden naam, publieke sleutel, effectieve datum, referentie (sleutel ID), serienummer, samenvattingsalgoritme, samenvatting, versie, afgever en E-postadres uit naar het opslaan bestand	Sleutelindex
UI	Vervang de sleutel	Sleutelindex
Sleutelindex	Lees de sleutelinformatie in van het bestand	Sleutelindex
Sleutelindex	Werk de sleutelinformatie bij	Database
UI	Geef een voltooiingsbericht weer	UI
UI	Geef de lijst opnieuw weer	UI

Kopieer handelspartner publieke sleutel van diskbestand naar een nieuwe sleutel

De gebruiker dient in te loggen en het certificaatbeheerhoofdmenu te activeren alvorens tot deze functie te komen.

Neem aan dat het bestand in X.509 formaat is.

Initiator	Actie	Deelnemer
Gebruiker	Roep de opnieuw opslaan van diskfunctie op	Gebruiker
UI	Geef een scherm weer om te vragen voor de sleutel ID en invoeren bestandsnaam	UI
Gebruiker	Toets de sleutel ID en bestandsnaam in	Gebruiker
Sleutelindex	Lees de sleutelinformatie in van het bestand	Sleutelindex
Sleutelindex	Bereken de certificaatsamenvatting	Samenvattingcalculator
Sleutelindex	Verifieer de samenvattingsovereenkomst	Sleutelindex

Initiator	Actie	Deelnemer
Sleutelindex	Schrijf de sleutelinformatie	Database
UI	Voeg de sleutel toe aan de lijst	UI
UI	Geef de lijst opnieuw weer	UI

Activeer handelspartnerovereenkomstbeheer hoofdmenu

Initiator	Actie	Deelnemer
Gebruiker	Spreek handelspartnerovereenkomstknop aan	Gebruiker
UI	Verkrijg een lijst van handelspartnerovereenkomst	Handelspartnerovereenkomstlijst
UI	Geef de lijst van handelspartnerovereenkomst op scherm weer	UI

Toevoeging handelspartnerovereenkomst

De gebruiker dient in te loggen en handelspartnerbeheerhoofdmenu te activeren alvorens tot deze functie te komen.

Initiator	Actie	Deelnemer
Gebruiker	Spreek de toevoegen handelspartnerovereenkomstknop aan	Gebruiker
UI	Geef handelspartnerovereenkomstscherm weer om lokale handelspartner en certificaat ID; op afstand gelegen handelspartner en certificaat ID te accepteren	UI
Gebruiker	Roep toevoegen nieuwe lokale handelspartner op	Gebruiker
UI	Geef een toevoegen handelspartnerscherm weer	UI
Gebruiker	Toets naam, contact, contact e-postadres, telefoon, fax, adres, volledige naam, commentaar in	Gebruiker
UI	Verifieer dat de handelspartner niet bestaat	Handelspartnerlijst
UI	Voeg de handelspartner toe	Handelspartnerlijst
UI	Geef de lokale handelspartner op scherm weer	UI
Gebruiker	Toets omhullingstype, seperatoren, kwalificerend element en ID in	Gebruiker
Gebruiker	Roep toevoegen nieuwe op afstand gelegen handelspartner op	Gebruiker
UI	Geef een toevoegen handelspartnerscherm weer	UI
Gebruiker	Toets naam, contact, contact e-postadres, telefoon, fax, adres, volledige naam, commentaar in	Gebruiker
UI	Verifieer dat handelspartner niet bestaat	Handelspartnerlijst
UI	Voeg de handelspartner toe	Handelspartnerlijst

Initiator	Actie	Deelnemer
UI	Geeft de op afstand gelegen handelspartner op scherm weer	UI
Gebruiker	Roep de binnenkomende routeringknop aan	Gebruiker
UI	Geef binnenkomende routeringsinformatiescherm weer	UI
Gebruiker	Toets binnenkomende informatie-status; veiligheid- NRO, NRR, en vertrouwelijkheid in; opslaan om EDI gegevens te ontvangen, geef opdracht om te lopen na ontvangst	Gebruiker
UI	Verifieer binnenkomende routeringsinformatie	Binnenkomende routering
UI	Voeg binnenkomende routering toe	Binnenkomende routering
Gebruiker	Spreek de uitgaande routeringsknop aan	Gebruiker
UI	Geeft uitgaande routeringsinformatiescherm weer	UI
Gebruiker	Toets transportinformatie-MIME ontvanger en zender e-postadres, maximale berichtafmeting, karakterset in	Gebruiker
Gebruiker	Toets veiligheids-NRO, NRR, vertrouwelijkheid in	Gebruiker
Gebruiker	Toets herverzendinginterval en actie in	Gebruiker
UI	Verifieer uitgaande routeringsinformatie	Uitgaande routering
UI	Voeg uitgaande routering toe	Uitgaande routering
UI	Geef het handelspartnerovereenkomst-hoofdscherm opnieuw weer	UI
Gebruiker	Selecteer om handelspartnerovereenkomst op te slaan	Gebruiker
UI	Voeg de handelspartnerovereenkomst toe	Handelspartnerovereenkomstlijst

Verander handelspartnerovereenkomst

De gebruiker dient in te loggen en handelspartner-beheerhoofdmenu te activeren alvorens tot deze functie te komen.

Initiator	Actie	Deelnemer
Gebruiker	Selecteer handelspartnerovereenkomst voor verandering	Gebruiker
Gebruiker	Spreek de verander handelspartnerovereenkomstknop aan	Gebruiker
UI	Verkrijg de geselecteerde handelspartnerovereenkomst	Handelspartnerovereenkomstlijst
UI	Verkrijg informatie-lokale en op afstand gelegen handelspartner, binnenkomende en uitgaande informatie	Handelspartnerovereenkomst
UI	Geef handelspartnerovereenkomstinformatie op scherm weer en sta niet toe om de lokale en op afstand gelegen handelspartner te veranderen	UI

Initiator	Actie	Deelnemer
Gebruiker	Verzoek om de lokale handelspartnerinformatie te veranderen	Gebruiker
UI	Verkrijg informatie omtrent de lokale handelspartner	Handelspartner
UI	Geeft de handelspartner informatie op scherm weer	UI
Gebruiker	Verander e-postadres van de handelspartner	Gebruiker
UI	Werk de handelspartner bij	Handelspartner
UI	Geef het handelspartnerovereenkomstscherm weer	UI
Gebruiker	Selecteer om de op afstand gelegen handelspartner te veranderen	UI
UI	Verkrijg informatie omtrent de op afstand gelegen handelspartner	Handelspartner
UI	Geef de handelspartnerinformatie op scherm weer	UI
UI	Geef het handelspartnerovereenkomstscherm weer	UI
Gebruiker	Verander het adres van de handelspartner	Gebruiker
UI	Werk de handelspartner bij	Handelspartner
UI	Geef het handelspartnerovereenkomstscherm weer	UI
Gebruiker	Verander de binnenkomende en uitgaande routeringsinformatie	Gebruiker
Gebruiker	Selecteer om de handelspartnerovereenkomst bij te werken	Gebruiker
UI	Werk de handelspartnerovereenkomst bij	Handelspartnerlijst

Verwijder handelspartnerovereenkomst

De gebruiker dient in te loggen en het handelspartnerovereenkomsthoofdmenu te activeren alvorens tot deze functie te komen.

Initiator	Actie	Deelnemer
Gebruiker	Selecteer een handelspartnerovereenkomst voor verwijdering	Gebruiker
Gebruiker	Spreek de verwijder handelspartnerovereenkomstknop aan	Gebruiker
UI	Verkrijg de geselecteerde handelspartnerovereenkomst	Handelspartnerovereenkomstlijst
UI	Verkrijg informatie - lokale en op afstand gelegen handelspartner	Handelspartnerovereenkomst
UI	Geef handelspartnerovereenkomstinformatie op scherm weer	UI
UI	Geef het bevestigingsscherm weer	UI
Gebruiker	Bevestig verwijdering	Gebruiker

Initiator	Actie	Deelnemer
UI	Verwijder handelspartnerovereenkomst	Handelspartnerovereenkomstlijst
UI	Verwijder de overeenkomst uit de lijst op scherm	UI
UI	Geeft de nieuwe lijst opnieuw op scherm weer	UI

Kopieer handelspartnerovereenkomst naar diskbestand

De gebruiker dient in te loggen en het handelspartnerovereenkomsthoofdmenu te activeren alvorens tot deze functie te komen.

Initiator	Actie	Deelnemer
Gebruiker	Selecteer een handelspartnerovereenkomst	Gebruiker
Gebruiker	Roep de kopieer naar diskfunctie op	Gebruiker
UI	Geef een scherm weer om te vragen voor de uitvoerbestandsnaam	UI
Gebruiker	Toets de bestandsnaam in	Gebruiker
UI	Geef een vervangingsbevestigingsscherm weer	UI
Gebruiker	Selecteer om het bestaande bestand over te schrijven	Gebruiker
UI	Voer de handelspartnerovereenkomst naar bestand uit als een flatfile	Handelspartnerovereenkomst
UI	Geef een voltooiingsbericht weer	UI
UI	Geef de lijst opnieuw weer	UI

Kopieer handelspartnerovereenkomst van diskbestand

De gebruiker dient in te loggen en het handelspartnerovereenkomsthoofdmenu te activeren alvorens tot deze functie te komen.

Initiator	Actie	Deelnemer
Gebruiker	Roep de kopieer van diskfunctie op	Gebruiker
UI	Geef een scherm weer om te vragen voor de invoerbestandsnaam	UI
Gebruiker	Toets de bestandsnaam in	Gebruiker
UI	Geef een vervangingsbevestigingsscherm weer	UI
Gebruiker	Selecteer om de bestaande handelspartnerovereenkomst over te schrijven	Gebruiker
UI	Vervang de handelspartnerovereenkomst	Handelspartnerovereenkomst
Handelspartnerovereenkomst	Lees de handelspartnerovereenkomstinformatie van het bestand in	Handelspartnerovereenkomst

Initiator	Actie	Deelnemer
Handelspartnerovereenkomst	Werk de handelspartnerovereen-komstinformatie bij	Database
UI	Geef een voltooiingsbericht weer	UI
UI	Geef de lijst opnieuw weer	UI

MIME Pakkettering

Initiator	Actie	Deelnemer
Authenticatie-agent	Creëer een MIME Object met EDI uitwisse-ling, AUTACK, handelspartnerovereenkomst	MIME-pakketteringsinrich-ting
MIME-pakketterings-inrichting	Verkrijg kwalificerend element en ID van zender en ontvanger	EDI uitwisseling
MIME-pakketterings-inrichting	Verkrijg van en naar e-postadres, maxim-ale MIME deelafmeting	Handelspartnerovereenkomst
MIME-pakketterings-inrichting	Verkrijg handelspartnerveiligheids- co-deringswerkwijze (bijvoorbeeld DES of RC4), handelspartner publieke sleutel ID, vertrouwelijkheidsvlag	Handelspartnerovereenkomst
MIME-pakketterings-inrichting	Omhullings EDI uitwisseling in PKCS om-hulling	PKCS omhullingsinrichting
MIME-pakketterings-inrichting	Creëer EDI lichaamsdeel voor de gePKCSte EDI uitwisseling	MIME lichaamsdeel
MIME-pakketterings-inrichting	Creëer AUTACK lichaamsdeel	MIME lichaamsdeel
MIME-pakketterings-inrichting	Creëer MIME kop- van en naar e-postadres	MIME kop
MIME-pakketterings-inrichting	Creëer MIME-delen van de MIME kop en lichaamsdelen	MIME bericht
MIME-pakketterings-inrichting	Retourneer het MIME bericht naar authen-ticatie-agent	MIME pakketteringsinrich-ting

MIME Ontpakkettering

Initiator	Actie	Deelnemer
Verzendpost	Creëer een MIME deel ogenblik	MIME-pakketterings-inrichting
MIME-pakketterings-inrichting	Log deel aankomst	auditlog
MIME-pakketterings-inrichting	Stel delen samen	MIME-pakketterings-inrichting
MIME-pakketterings-inrichting	Log alle ontvangen delen	auditlog
MIME-pakketterings-inrichting	Pak gePKCSte lichaamsdeel uit	PKCS ont-omhullings-inrichting
MIME-pakketterings-inrichting	Informeer authenticatie-agent post aankomst	MIME-pakketterings-inrichting
Authenticatie-agent	Verkrijg van en naar e-postadres	MIME-pakketterings-inrichting

Initiator	Actie	Deelnemer
MIME-pakketterings-inrichting	Verkrijg TP veiligheid	Handelspartner-overeenkomst
Authenticatie-agent	Verkrijg lijst van lichaamsdelen	MIME-bericht
Authenticatie-agent	Verkrijg AUTACK lichaamsdeel	MIME-bericht
Authenticatie-agent	Verkrijg EDI uitwisseling	MIME-bericht
Authenticatie-agent	Ga door met andere verwerking	Authenticatie-agent

PKCS Pakkettering

Initiator	Actie	Deelnemer
MIME-pakketterings-inrichting	Creëer een gePCKSte EDI uitwisseling	PKCS pakketterings-inrichting
PKCS-pakketterings-inrichting	Verkrijg kwalificerend element en ID van zender en ontvanger	EDI uitwisselings-inrichting
PKCS-pakketterings-inrichting	Verkrijg publieke sleutel ID en code-ringswerkwijze voor handelspartner (b.v. DES of RC4)	Handelspartnerover-eenkomst
PKCS-pakketterings-inrichting	Verkrijg publieke sleutel van handelspartner	Sleutelindex
PKCS-pakketterings-inrichting	Verkijg willekeurige DES sleutel	DES coderings-inrichting
PKCS-pakketterings-inrichting	Codeer de EDI uitwisseling	DES coderings-inrichting
PKCS-pakketterings-inrichting	Codeer de DES sleutel	BSAFE
PKCS-pakketterings-inrichting	Creëer het gePKCSte MIME lichaamsdeel met de gecodeerde DES sleutel en EDI uitwisseling	MIME lichaamsdeel
PKCS-pakketterings-inrichting	Retourneer de gePKCSte EDI uitwisseling	PKCS-pakketterings-inrichting

PKCS Ontpakkettering

Initiator	Actie	Deelnemer
MIME-pakketterings-inrichting	Pak een gePKCSte lichaamsdeel uit	PKCS pakketterings-inrichting
PKCS-pakketterings-inrichting	Verkrijg publieke sleutel ID van handelspartner	Handelspartnerover-eenkomst
PKCS-pakketterings-inrichting	Verkrijg publieke sleutel van handelspartner	Sleutelindex
PKCS-pakketterings-inrichting	Pas het certificaat in de omhulling aan aan het certificaat en de sleutelindex	Publieke sleutel van de handelspart-ner
PKCS-pakketterings-inrichting	Verkrijg de gePKCSte EDI uitwisselingsinrichting	gePKCSte lichaams-deel
PKCS-pakketterings-inrichting	Decodeer de DES sleutel	BSAFE

Initiator	Actie	Deelnemer
PKCS-pakketterings-inrichting	Decodeer de gecodeerde EDI uitwisseling	DES coderings-inrichting
PKCS-pakketterings-inrichting	Retourneer de EDI uitwisselingsinrichting naar MIME pakketteringsinrichting	PKCS-pakketterings-inrichting

Werk met volgbestand

Initiator	Actie	Deelnemer
Gebruiker	Roep werk met volgbestandfunctie op	Gebruiker
UI	Vraag voor selectiecriteria - datumbereik, zender/-ontvanger, volgbestand ID, status, gegevenstype, uitwisselingsstuurgetal (gegevenstype gevoelig en uitsluitend toepassen op EDI gegevens)	UI
Gebruiker	Toets criteria in bijvoorbeeld datumbereik	Gebruiker
UI	Verkrijg een lijst van volgbestanden die binnen het gespecificeerde datumbereik liggen	Volgbestand
Volgbestand	Databasegegevens opvraag	Database
UI	Geef een lijst van volgbestanden weer	UI
Gebruiker	Roep kijkdetail op van een EDI groep	Gebruiker
UI	Verkrijg detail	Volgbestand
UI	Geef het detail van de EDI groep weer	UI
Gebruiker	Roep de herverzending van een uitwisseling op	Gebruiker
UI	Herverzending van de uitwisseling	Authenticatie-agent
UI	Geef het detail opnieuw weer	UI
Gebruiker	Afsluiten	Gebruiker
UI	Geef de lijst van volgbestand opnieuw weer	UI
Gebruiker	Selecteer om een EDI groep opnieuw uit te zenden	Gebruiker
UI	Herverzending van de groep	Authenticatie-agent
UI	Opnieuw weergeven van de lijst van volgbestand	UI
Gebruiker	Herbewerk een uitgaande groep	Gebruiker
UI	Herbewerk een uitgaande groep (begin bij het begin)	Authenticatie-agent
UI	Opnieuw weergeven van de lijst van volgbestand	UI
Gebruiker	Herbewerk een binnenkomende groep	Gebruiker
UI	Herbewerk een binnenkomende groep (begin bij het begin)	Authenticatie-agent
UI	Opnieuw weergeven van de lijst van volgbestand	UI
Gebruiker	Ga door van laatste actie	Gebruiker
UI	Vervolg laatste actie	Authenticatie-agent

Initiator	Actie	Deelnemer
Authenticatie-agent	Verkrijg status	Volgbestand
Authenticatie-agent	Vervolg proces volgens de status	Authenticatie-agent
UI	Opnieuw weergeven van de lijst van volgbestand	UI
Gebruiker	Herhaal laatste actie van een succes binnenkomende groep dat is hervertalen	Gebruiker
UI	Herhaal laatste actie	Authenticatie-agent
Authenticatie-agent	Verkrijg status	Volgbestand
Authenticatie-agent	Herhaal laatste actie	Authenticatie-agent
UI	Opnieuw weergeven van de lijst van volgbestand	UI
Gebruiker	Selecteer om een groep van volgbestand te printen	Gebruiker
UI	Verkrijg volgbestand samenvattingsinformatie	Volgbestand
UI	Formatteer het rapport	UI
UI	Druk het rapport af	Printer
UI	Opnieuw weergeven van de lijst van volgbestand	UI
Gebruiker	Geef een vasthoud EDI-groep vrij	Gebruiker
UI	Verander de status van het volgbestand om vrij te geven	Volgbestand
UI	Verwerk de EDI groep	Authenticatie-agent
UI	Opnieuw weergeven van de lijst van volgbestand	UI
Gebruiker	Selecteer om inhoud van een ontvangen post weer te geven	Gebruiker
UI	Verkrijg de postinhoud	Volgbestand
Volgbestand	Verkrijg de postinhoud	Postbestand
UI	Geef de post weer	UI
Gebruiker	Afsluiten	Gebruiker
UI	Opnieuw weergeven van de lijst van volgbestand	UI

Bewaak serverbewerkingen

Initiator	Actie	Deelnemer
Gebruiker	Roep werk met bewaakserverbewerkingsfunctie op	Gebruiker
UI	Verkrijg serverbewerkingeninformatie	Besturingssysteem op de server
UI	Geef de serverbewerkingnaam, status weer	UI
Gebruiker	Selecteer om de status te vernieuwen	Gebruiker
UI	Verkrijg serverbewerkingeninformatie	Besturingssysteem op de server
UI	Geef de serverbewerking naam, status weer	UI
Gebruiker	Selecteer om een serverbewerking te starten bijvoorbeeld bewaker	Gebruiker

1003644

Initiator	Actie	Deelnemer
UI	Start de serverbewerking	Bewerkingsconfiguratie
Bewerkings-configuratie	Start de bewerking	Besturingssysteem op de server
UI	Verkrijg serverbewerkingeninformatie	Besturingssysteem op de server
UI	Geef de serverbewerkingsnaam, status weer	UI

Ontvang een ongeldig EDI document met integriteitsprobleem

Neem aan dat het begin van het manuscript gelijk is aan Ontvang een geldig EDI document. Na verifiering van de samenvatting van het deel AUTACK analoog aan de gedecodeerde ondertekende samenvatting en het AUTACK, komt de authenticatie-agent te weten dat de samenvatting in het AUTACK niet overeenkomt met de samenvatting van de EDI uitwisseling.

Initiator	Actie	Deelnemer
Authenticatie-agent	Creëer een uitwisselingsintegriteitsfoutlog met volgende informatie: samenvatting in AUTACK, samenvatting van de EDI uitwisseling, AUTACK stuurgetal, uitwisselingsstuurgetal, handelspartnernaam, volgbestand ID.	Auditlog
Authenticatie-agent	Werk de status bij van het volgbestand om integriteitsfout uit te wisselen	Volgbestand
Authenticatie-agent	Verkrijg lokaal e-postadres	Handelspartnerovereenkomst
Authenticatie-agent	Formateer een uitwisselingsintegriteitsfout e-post met volgende informatie: tijdstempel, samenvatting in AUTACK, samenvatting van de EDI uitwisseling, AUTACK stuurgetal, uitwisselingsstuurgetal, handelspartnernaam, volgbestand ID	Authenticatie-agent
Authenticatie-agent	verzend de e-post	verzend post
Authenticatie-agent	Verkrijg EDI uitwisselingscreatiedatum en tijd	EDI uitwisseling
Authenticatie-agent	Formateer een negatieve AUTACK- de samenvatting in het ontvangen AUTACK	AUTACK
Authenticatie-agent	Creëer een AUTACK uitwisseling	AUTACK uitwisseling
Authenticatie-agent	Codeer het negatieve AUTACK in MIME formaat	MIME-pakketteringsinrichting
Authenticatie-agent	Verzend het gecodeerde negatieve AUTACK naar handelspartner	Verzendpost
Authenticatie-agent	Werk de status bij van het volgbestand om integriteitsfout met verzonden negatief AUTACK uit te wisselen	Volgbestand
Authenticatie-agent	Log het verzonden negatieve AUTACK gebeurtenis	Audit log

Ontvang een AUTACK met een integriteitsprobleem

Neem aan dat het begin van het manuscript gelijk is aan het Ontvang een geldig EDI document. De authenticatie-agent komt te weten dat de samenvatting van het deel AUTACK niet gelijk is aan de gecodeerde ondertekende samenvatting en AUTACK.

Initiator	Actie	Deelnemer
Authenticatie-agent	Creëer een AUTACK integriteitsfoutlog met volgende informatie: ondertekende samenvatting van het deel AUTACK in AUTACK, gedecodeerde ondertekende samenvatting van het deel AUTACK in AUTACK, berekende samenvatting van het deel AUTACK, AUTACK stuurgetal, handelspartnernaam, handelspartner publieke sleutel, volgbestand ID	Auditlog
Authenticatie-agent	Werk de status bij van het volgbestand naar AUTACK integriteitsfout	Volgbestand
Authenticatie-agent	Verkrijg lokaal e-postadres	Handelspartnerovereenkomst
Authenticatie-agent	Formateer een AUTACK integriteitsfout e-post met volgende informatie: tijdstempel, ondertekende samenvatting van het deel AUTACK in AUTACK, gedecodeerde ondertekende samenvatting van het deel AUTACK in AUTACK, berekende samenvatting van het deel AUTACK, AUTACK stuurgetal, handelspartnernaam, publieke sleutel van handelspartner, volgbestand ID.	Authenticatie-agent
Authenticatie-agent	Verzend de e-post	Verzendpost

Ontvang niet-ondersteunde post

Neem aan dat het begin van het manuscript gelijk is aan het Ontvang een geldig EDI document. De authenticatie-agent komt te weten dat de post niet een EDI document is, niet een AUTACK, en niet een certificaat.

Initiator	Actie	Deelnemer
Authenticatie-agent	Dump de niet ondersteunde post naar een bestand	Dumpbestand
Dumpbestand	Verkrijg de dumpbestandindex	Configuratie
Dumpbestand	Creëer een unieke dumpbestandnaam	Dumpbestand
Dumpbestand	Voer de niet-ondersteunde post uit naar het dumpbestand	Dumpbestand
Authenticatie-agent	Creëer een ontvangen niet-ondersteunde postfoutlog met volgende informatie: zender en ontvanger e-postadres, onderwerp, e-postbericht ID, dumpbestandnaam	Auditlog
Authenticatie-agent	Werk de status bij van het volgbestand naar ontvangen niet ondersteunde post, sla de dumpbestandnaam op	Volgbestand
Authenticatie-agent	Verkrijg lokaal e-postadres	Handelspartnerovereenkomst

Initiator	Actie	Deelnemer
Authenticatie-agent	Formatteer een ontvangen niet-ondersteunde postfout e-post met volgende informatie: zender en ontvanger e-postadres, onderwerp, e-postbericht ID, een bestandsnaam	Authenticatie-agent
Authenticatie-agent	Verzend de e-post	Verzendpost

Ontvang een EDI uitwisseling zonder AUTACK terwijl niet-afwijzing van oorsprong verwacht wordt

Neem aan dat het begin van het manuscript gelijk is aan het Ontvang een geldig EDI document. De authenticatie-agent komt te weten dat er geen AUTACK in de post is.

Initiator	Actie	Deelnemer
Authenticatie-agent	Dump de EDI uitwisseling naar een bestand	Dumpbestand
Dumpbestand	Verkrijg de dumpbestandindex	Configuratie
Dumpbestand	Wek een unieke dumpbestandsnaam op	Dumpbestand
Dumpbestand	Voer de EDI uitwisseling uit naar het dumpbestand	Dumpbestand
Authenticatie-agent	Creëer een AUTACK niet ontvangen foutlog met volgende informatie: tijdsstempel, uitwisselingsstuurgetal, handelspartnernaam, volgbestand ID, dumpbestandnaam	Auditlog
Authenticatie-agent	Werk de status bij van het volgbestand naar AUTACK niet-ontvangen, sla de dumpbestandnaam op	Volgbestand
Authenticatie-agent	Verkrijg lokaal e-postadres	Handelspartnerovereenkomst
Authenticatie-agent	Formateer een AUTACK niet-ontvangen fout e-post met volgende informatie: tijdsstempel, uitwisselingstuurgetal, handelspartnernaam, volgbestand ID, dumpbestandnaam	Authenticatieagent
Authenticatie-agent	Verzend de e-post	Verzendpost

Ontvang een onverwacht AUTACK

Neem aan dat het begin van het manuscript gelijk is aan het Ontvang een geldig EDI document. De authenticatie-agent komt te weten dat er een AUTACK in de post is, nadat de handelspartnerovereenkomst geen niet-afwijzing van oorsprong specificeert.

Initiator	Actie	Deelnemer
Authenticatie-agent	Dump de EDI uitwisseling in een bestand	Dumpbestand
Dumpbestand	Verkrijg de dumpbestandindex	Configuratie
Dumpbestand	Wek een unieke dumpbestandnaam op	Dumpbestand
Dumpbestand	Voer de EDI uit naar het dumpbestand	Dumpbestand

Initiator	Actie	Deelnemer
Authenticatie-agent	Dump de AUTACK uitwisseling naar een bestand	Dumpbestand
Dumpbestand	Verkrijg de dumpbestandindex	Configuratie
Dumpbestand	Wek een unieke dumpbestandnaam op	Dumpbestand
Dumpbestand	Voer de AUTACK uit naar het dumpbestand	Dumpbestand
Authenticatie-agent	Creëer een onverwachte AUTACK foutlog met volgende informatie: tijdsstempel, uitwisselingsstuurnummer, handelspartnernaam, volgbestand ID, dumpbestandnamen	Auditlog
Authenticatie-agent	Werk de status bij van het volgbestand naar onverwacht AUTACK, sla de dumpbestandnamen op	Volgbestand
Authenticatie-agent	Verkrijg lokaal e-postadres	Handelspartnerovereenkomst
Authenticatie-agent	Formatteer een onverwacht AUTACK fout e-post met volgende informatie: tijdsstempel, uitwisselingsstuurgetal, handelspartnernaam, volgbestand ID, dumpbestandnamen	Authenticatie-agent
Authenticatie-agent	Verzend de e-post	Verzend post

Figuren 14-41 illustreren de verscheidene schermdisplays, in een conventioneel WINDOWS type omgeving, die in staat zijn tot het bij voorkeur weergegeven worden op de typische computerschermen 116, 118 geassocieerd met de servers 112, 114 bij het uitvoeren van de bovenbeschreven werkwijze onder besturing van het programma dat gebaseerd is op de manuscripten van tabel A. In dit opzicht, toont figuur 14 het algehele schermdisplay dat gepresenteerd wordt aan de partijen op het netwerk die in aanmerking komen om deel te nemen in een compagnon-tot-compagnon, computer-tot-computer, zaken EDI transacties over het INTERNET. Zoals bij wijze van voorbeeld getoond in figuur 14, kan de gebruiker bij wijze van voorbeeld gepresenteerd worden met de keuze om WINDOWS te selecteren voor HANDELSPARTNERPROFIELEN, HANDELSPARTNEROVEREENKOMSTEN, SLEUTELBEHEER, en VOLGEN in de conventionele WINDOWS omgeving die bij voorkeur gebruikt wordt.

Figuren 15-21 tonen verscheidene computerschermdisplays die aan de gebruiker gepresenteerd kunnen worden na het selecteren van het HANDELSPARTNERPROFIELEN venster in het schermdisplay van figuur 14. Figuur 15 representeert

een scenario van drie mogelijke handelspartners geïdentificeerd als CISCO, SEARS, en ME, waar ME de gebruiker zelf representeert. Figuur 16 toont een mogelijke dialoogdoos voor het creëren van het handelspartnerprofiel rechtstreeks op het computerscherm 116, 118. Analoog, toont figuur 17 een mogelijke dialoogdoos voor het creëren van contactinformatie voor de handelspartner rechtstreeks op het computerscherm 116, 118. Figuur 18 toont een mogelijke dialoogdoos voor het creëren van EDI kwalificerend elementinformatie rechtstreeks op het computerscherm 116, 118. Figuur 19 toont een mogelijke dialoogdoos voor handelspartner gebonden sleutels die weergegeven worden en veranderd kunnen worden rechtstreeks op het computerscherm 116, 118, waarbij twee opties voor Binden en Ontbinden getoond worden. Figuur 20 toont het computerschermdisplay 116, 118 wanneer de BINDEN SLEUTELS optie geselecteerd is in het display van figuur 19 teneinde een bepaalde sleutel te verbinden met een bepaalde handelspartner. Figuur 21 toont het computerschermdisplay 116, 118 voor SLEUTEL ADDENDUM voor, bij wijze van voorbeeld, het displayen van een geformatteerd certificaat dat gebonden kan worden aan de handelspartner samen met de sleutel.

Figuren 22-28 tonen verscheidene computerschermdisplays die aan de gebruiker gepresenteerd kunnen worden na het selecteren van het HANDELSPARTNEROVEREENKOMSTEN venster in het schermdisplay van figuur 14. Figuur 22 representeert een scenario van dezelfde drie handelspartners zoals geïdentificeerd in figuur 15. Figuur 23 toont een dialoogdoos voor het creëren, in het bovengenoemde voorbeeld, van een handelspartnerovereenkomst tussen de gebruiker ME, die de lokale ID is, en SEARS, die de op afstand gelegen ID is, rechtstreeks op het computerscherm 116, 118. Figuur 24 toont een dialoogdoos voor het creëren van binnenkomende routeringsinstructies voor de handelspartnerovereenkomst rechtstreeks op het computerscherm 116, 118. Analoog, tonen figuren 25-27 verscheidene dialoogdozen voor het creëren van uitgaande routeringsinstructies voor

de handelspartnerovereenkomst rechtstreeks op het computerscherm 116, 118. Figuur 28 toont een dialoogdoos voor het selecteren van uitgaande herverzending rechtstreeks op het computerscherm 116, 118.

Figuren 29-33 tonen verscheidene computerscherm-displays die aan de gebruiker gepresenteerd kunnen worden na het selecteren van het SLEUTELBEHEERvenster in het schermdisplay van figuur 14. Figuur 29 representeert opnieuw een scenario van dezelfde drie handelspartners zoals gepresenteerd in figuur 15. Figuur 30 toont een mogelijke dialoogdoos geassocieerd met de lokale sleutel ID, Figuur 31 toont een mogelijke dialoogdoos geassocieerd met de op afstand gelegen sleutel ID, Figuur 32 toont een mogelijke dialoogdoos geassocieerd met sleuteldetails, en Figuur 33 toont een mogelijke dialoogdoos geassocieerd met export van de publieke sleutel naar een ander bestand.

Figuren 34-41 tonen verscheidene computerscherm-displays die aan de gebruiker getoond kunnen worden na het selecteren van het VOLGvenster in het schermdisplay van Figuur 14. Figuur 34 toont een schermdisplay op het computerscherm 116, 118 waarin twee EDI berichten verzonden zijn, één tussen SEARS en CISCO, en één tussen ME en ZIJ, bij wijze van voorbeeld. Figuur 35 toont een mogelijk display op het computerscherm 116, 118 van de uitwisselingen tussen de handelspartners en toont de niet-afwijzing van ontvangst AUTACK, tonende de AUTACK status op het computerscherm 116, 118 in overeenstemming met de onderhavige uitvinding. Figuur 36 toont een mogelijk display op het computerscherm 116, 118 van de EDI gegevens nadat de KIJK EDI GEGEVENS dialoogdoos geselecteerd is in het schermdisplay van figuur 35. Figuren 37-38 tonen mogelijke schermdisplays op een computerscherm 116, 118 voor het selecteren van volgcriteria. Figuur 39 toont een mogelijk schermdisplay op een computerscherm 116, 118 van een auditloog, waarbij figuren 40-41 mogelijke schermdisplays op het computerscherm 116, 118 tonen voor het selecteren van auditloog selectiecriteria.

Verwijzende nu naar figuur 2, zal nu het bevoorkeurde proces van authenticatie en niet-afwijzing van oorsprong in overeenstemming met de thans bevoorkeurde werkwijze van de onderhavige uitvinding beschreven worden. Zoals getoond en bevoorkeurd in figuur 2, representeert blok 200 een typische EDI uitwisseling in overeenstemming met de onderhavige uitvinding. Blok 202 representeert de bevoorkeurde actie van de server bij het zendereinde ten opzichte van de EDI uitwisseling in overeenstemming met de werkwijze van de onderhavige uitvinding. Zoals getoond en bevoorkeurd, berekent de zenderserver bij voorkeur de MD5 voor de gehele EDI uitwisseling, zoals van ISA tot het laatste karakter IEA (MD5EDIINTERCHANGE genoemd). Deze waarde wordt vervolgens bij voorkeur ingevoerd in een voorafbepaalde positie in het AUTACK bericht, zoals bij voorkeur het tweede element van segment USY in het AUTACK bericht. De zenderserver berekent vervolgens bij voorkeur de MD5 van het AUTACK bericht, zoals bij voorkeur van het eerste karakter van USH tot het eerste karakter van UST. De zenderserver ondertekent vervolgens bij voorkeur het AUTACK door de MD5 te coderen met de privesleutel van de zender. Deze berekende waarde wordt vervolgens bij voorkeur ingevoerd in een voorafbepaalde positie in het AUTACK, zoals bij voorkeur als het eerste element van segment USR in het AUTACK bericht. Blok 204 representeert een typisch AUTACK bericht in overeenstemming met de bevoorkeurde werkwijze van de onderhavige uitvinding nadat de zenderservers de actie genomen heeft geïllustreerd in blok 202. Het AUTACK 204 wordt vervolgens bij voorkeur verzonden naar de ontvangerserver waar de ontvangeractie en verificatie geïllustreerd in blok 206 bij voorkeur plaatsvindt. Indien de EDI uitwisseling gecodeerd is, dan decodeert de ontvangerserver deze bij voorkeur en berekent de MD5 van de ontvangen EDI uitwisseling. Aannemende dat niet-afwijzing van oorsprong gewenst of gevraagd is, dan decodeert de ontvangerserver bij voorkeur, onder gebruikmaking van de publieke sleutel van de zender, de inhoud van het eerste element van het USR

segment in het AUTACK bericht 204, dat de plaats is waar de zenderserver de MD5 van het AUTACK ingevoegd heeft. De waarde die aldus verkregen wordt door de decodering is de MD5 van het AUTACK bericht, in het bovengenoemde voorbeeld, van het eerste karakter van USH tot het eerste karakter van UST. De ontvangerserver berekent vervolgens bij voorkeur de MD5 van het AUTACK bericht en vergelijkt de berekende MD5 met de waarde van de MD5 verkregen door de decodering van de inhoud van het eerste element van het USR segment en het AUTACK bericht. Indien beide waarden van MD5 gelijk zijn, dan weet de ontvangerserver dat de integriteit van het AUTACK behouden is en niet-afwijzing van oorsprong tot stand gebracht is. De ontvangerserver vergelijkt vervolgens bij voorkeur de MD5 van de EDI uitwisseling met de MD5 in het USY segment van het AUTACK bericht, dat de plaats is waar de zenderserver de MD5 van de EDI uitwisseling ingevoegd heeft, en, indien de twee MD5 waarden gelijk zijn, weet de ontvangerserver dat de integriteit van de EDI uitwisseling behouden is, authenticiteit geverifieerd is, en niet-afwijzing van oorsprong tot stand gebracht is.

Verwijzende nu naar Figuur 3, zal het bevoorkeurde proces van niet-afwijzing van ontvangst en overeenstemming met de thans bevoorkeurde werkwijze van de onderhavige uitvinding beschreven worden. Zoals getoond en bevoorkeurd in blok 208, is de actie van de ontvangerserver bij het verifiëren van de integriteit en authenticiteit van de ontvangen EDI uitwisseling bij voorkeur zoals boven beschreven met betrekking tot blok 206 van Figuur 2. Daarna, creëert de ontvangerserver bij voorkeur een nieuwe AUTACK, zoals het AUTACK bericht weergegeven door blok 210, en zendt het nieuwe AUTACK 210 naar de zenderserver voor verificatie door de originele zenderserver, zoals gerepresenteerd door blok 212. Zoals getoond en bevoorkeurd in Figuur 3, bij het creëeren van het AUTACK, bezet de ontvangerserver bij voorkeur alle segmenten en elementen zoals geschikt, zoals alle segmenten en elementen tot en met UST. De ontvangerserver berekent dan bij voorkeur de MD5 van het

nieuwe AUTACK, zoals van USA tot het eerste karakter van UST, en ondertekent de berekende MD5 met de privesleutel van de ontvanger. De ontvangerserver voegt dan bij voorkeur de digitaal ondertekende MD5 in in een vooraf bepaalde plaats in het nieuwe AUTACK, zoals het eerste element van het USR segment. De ontvangerserver bezet vervolgens bij voorkeur de UNT en UNZ segmenten van het AUTACK zoals geschikt en verzendt het geprepareerde AUTACK naar de originele zenderserver. De originele zenderserver verifieert dan bij voorkeur de digitale ondertekening van het ontvangen AUTACK door dit te decoderen met de publieke sleutel van de ontvanger, waarbij dit door deze decodering verkregen waarde MD5 van het ontvangende AUTACK is. De originele zenderserver berekent vervolgens de MD5 van het ontvangen nieuwe AUTACK en vergelijkt dit met de waarde van MD5 verkregen van het decoderingsproces. Indien de twee waarden van MD5 gelijk zijn, dan weet de oorspronkelijke zenderserver dat de integriteit van het nieuwe AUTACK behouden is en niet-afwijzing van oorsprong van het nieuwe AUTACK tot stand gebracht is. De originele zenderserver weet tevens dat indien de MD5 bevat in het USY segment van het ontvangen nieuwe AUTACK in het bovengenoemde voorbeeld gelijk is aan MD5 van de eerder verzonden EDI uitwisseling en de bevestiging positief is (zoals bij voorkeur verkregen door het testen van de veiligheidscode in het nieuwe AUTACK bericht), dan is de EDI uitwisseling in kwestie bekend bij zowel de zender als ontvanger daar de MD5 van de EDI uitwisseling en het uitwisselingsgetal bevat zijn in het AUTACK bericht en geldig zijn herkend. Aanvullend, is de integriteit en authenticiteit van EDI uitwisseling na ontvangst geverifieerd en ontkent de ontvangerzender niet de EDI uitwisseling in kwestie ontvangen te hebben.

Verwijzende nu naar Figuren 4-5, wordt een processtroomdiagram van de thans bevoorkeurde werkwijze voor het ontvangen respectievelijk verzenden van E-post, in overeenstemming met de thans bevoorkeurde werkwijze van de onderhavige uitvinding getoond. In dit opzicht, zit TEMPLAR, de

regeleenheid voor het uitvoeren van de thans bevoorkeurde werkwijze van de onderhavige uitvinding, bij voorkeur tussen het conventionele bericht en de gebruiker gespecificeerde EDI flat-file op de zend- en ontvangsystemen, waarbij de conventionele VERZENDPOST geleverd met het UNIX X-WINDOWS OF MICROSOFT WINDOWS besturingssysteem bij voorkeur gebruikt wordt om post te verzenden en te ontvangen, waarbij de post die verzonden en bij voorkeur ontvangen wordt een MIME compliant is, en waarbij PKCS bij voorkeur gebruikt wordt om MIME gecodeerde lichaamsdelen te coderen en decoderen. Bij voorkeur, zijn de MIME identificatie-elementen niet gecodeerd.

Zoals boven opgemerkt, is het EDIFACT AUTACK bericht bij voorkeur gebruikt om veilige authenticatie, niet-afwijzing van oorsprong en/of ontvangst, en bevestiging of ontkenning van bevestiging voor één of meer X.12 EDIFACT omhullingen te leveren. Bij voorkeur, worden meerdere EDI omhullingen gezien als één blok gegevens in het systeem van de onderhavige uitvinding. Bij voorkeur, indien het een ontvangen AUTACK bericht aan berichtintegriteit ontbreekt, wordt een bevestiging van ontvangst niet teruggezonden naar de originele verzender van het bericht, hoewel, indien gewenst, het systeem eenvoudig gewijzigd kan worden om dit te bereiken.

Verwijzende nu naar Figuren 6-9, zijn deze processtroomdiagrammen met betrekking tot handelspartnerbeheer, audit log beheer, volgbeheer, respectievelijk bewerkingsbewaking, in overeenstemming met de thans bevoorkeurde werkwijze van de onderhavige uitvinding. Deze diagrammen zijn zelfuitleggend wanneer beschouwd samen met de voorgaande discussie en zullen hierna niet in groter detail beschreven worden.

Figuur 10 is een functioneel diagram van de organisatie van de thans bevoorkeurde werkwijze van de onderhavige uitvinding zoals gerepresenteerd door het manuscript van Tabel A en de voorgaande discussie en zal niet in grotere detail hierna beschreven worden.

Tot slot, bevatten Figuren 11-13 een processtroomdiagram van de thans bevoorkeurde werkwijze van de onderhavige uitvinding in overeenstemming met de voorgaande beschrijving, waarbij Figuur 11 verscheidene stappen toont van verificatie van de integriteit van het AUTACK, de EDI uitwisseling, en het certificaat, waarbij NRO niet-afwijzing van oorsprong representeert en NRR niet-afwijzing van ontvangst representeert. Figuur 12 toont het deel van de werkwijze gewijd aan TPA verwerking. Figuur 13 toont het deel van de werkwijze van de onderhavige uitvinding gewijd aan het verwerken van de publieke en privesleutels, alsmede TPA, bij het uitvoeren van de werkwijze van de onderhavige uitvinding zoals boven beschreven.

Aldus, wordt door het gebruik van het AUTACK bericht als een dokument voor de digitale ondertekening dat ondertekend is gebaseerd op een publieke/privesleutsysteem, zoals RSA, een efficiënt, in hoge mate veilige berichtgeving voor EDI over een open netwerk, zoals het INTERNET, verschaft waarin handelspartners eenvoudig veilige verificatie en authenticatie en niet-afwijzing van zowel oorsprong als ontvangst kunnen verkrijgen, hetgeen in het geheel belangrijk is in snel bewegende elektronica zakentransacties over een ruime verspreid geografisch gebied waarin een open netwerk het meest levensvatbare communicatiemedium is.

Geclaimd wordt:

C O N C L U S I E S

1. In een communicatiesysteem voor het selectief verbinden van een groot aantal computers over een open publiek netwerk waarover de computers veilige digitale berichten uitwisselen tussen een zendcomputer en een ontvangcomputer in het grote aantal computers, waarbij de zendcomputer een eerste geassocieerde publieke sleutel en een eerste geassocieerde privé sleutel heeft, waarbij de ontvangcomputer een tweede geassocieerde publieke sleutel en een tweede geassocieerde privé sleutel heeft, waarbij de digitale berichten een EDI uitwisselingscommunicatie bevatten tussen de zendcomputer en de ontvangcomputer, waarbij de EDI uitwisselingscommunicatie een geassocieerd EDI bevestigingsbericht heeft; waarbij de verbetering omvat

middelen voor het berekenen van een eerste hash voor de EDI uitwisselingscommunicatie van de zendcomputer;

middelen voor het invoegen van de eerste hash in een vooraf bepaalde plaats in het geassocieerde EDI bevestigingsbericht;

middelen voor het berekenen van een tweede hash van het geassocieerde EDI bevestigingsbericht;

middelen voor het digitaal ondertekenen van het geassocieerde EDI bevestigingsbericht, waarbij de middelen voor het digitaal ondertekenen van het bericht middelen bevatten voor het coderen van de tweede hash met de privé sleutel van de zendcomputer;

middelen voor het invoegen van de tweede hash in een vooraf bepaalde plaats in het geassocieerde EDI bevestigingsbericht;

middelen voor het verzenden van de EDI uitwisselingscommunicatie samen met het digitaal ondertekende geassocieerde EDI bevestigingsbericht naar de ontvangcomputer over het open publieke netwerk; en

middelen geassocieerd met de ontvangcomputer voor het ontvangen en bewerken van de ontvangen EDI uitwisselingscommunicatie en het digitaal ondertekende EDI bevestigingsbericht voor het verschaffen van authenticatie en niet-afwijzing van de EDI uitwisselingscommunicatie van de zendcomputer waarbij de middelen middelen omvatten voor het decoderen van de gecodeerde tweede hash met de publieke sleutel van de zendcomputer; waardoor veilige privé EDI uitwisselingscommunicaties over een open publiek netwerk kunnen optreden onder het verschaffen van authenticatie en niet-afwijzing van de EDI communicaties.

2. Een verbeterd veilig open netwerk communicatiesysteem volgens conclusie 1, waarin de middelen geassocieerd met de ontvangcomputer verder middelen bevatten voor het berekenen van een derde hash van het ontvangen EDI bevestigingsbericht; en middelen voor het vergelijken van de derde hash met de gedecodeerde tweede hash van het ontvangen EDI bevestigingsbericht, waarbij de vergelijkingsmiddelen middelen bevatten voor het verschaffen van een indicatie van de integriteit van het EDI bevestigingsbericht en niet-afwijzing van oorsprong wanneer de gedecodeerde tweede hash en de derde hash met elkaar overeenkomen.

3. Een verbeterd veilig open netwerk communicatiesysteem volgens conclusie 2, waarin de middelen geassocieerd met de ontvangcomputer verder middelen bevatten voor het berekenen van een vierde hash van de ontvangen EDI uitwisselingscommunicatie; en middelen voor het vergelijken van de vierde hash van de ontvangen EDI uitwisselingscommunicatie met de eerste hash in het ontvangen EDI bevesti-

gingsbericht, waarbij de vergelijkingsmiddelen middelen bevatten voor het verschaffen van een indicatie van integriteit en verificatie van authenticiteit van de EDI uitwisselingscommunicatie en niet-afwijzing van oorsprong wanneer de eerste en vierde hash met elkaar overeenkomen.

4. Een verbeterd veilig open netwerkcommunicatiesysteem volgens conclusie 3, waarin de middelen geassocieerd met de ontvangcomputer verder middelen bevatten voor het opwekken van een antwoord EDI bevestigingsbericht en het verzenden van het antwoord EDI bevestigingsbericht naar de zendcomputer over het open publieke netwerk, waarbij de middelen voor het opwekken van het antwoord EDI bevestigingsbericht middelen bevatten voor het berekenen van een vijfde hash van het antwoord EDI bevestigingsbericht en voor het digitaal ondertekenen van de vijfde hash door het coderen van de vijfde hash met de privé sleutel van de ontvangcomputer; en middelen voor het invoegen van de digitaal ondertekende vijfde hash in een vooraf bepaalde plaats in het verzonden antwoord EDI bevestigingsbericht.

5. Een verbeterd veilig open netwerkcommunicatiesysteem volgens conclusie 4, verder bevattende middelen geassocieerd met de zendcomputer voor het ontvangen van het verzonden antwoord EDI bevestigingsbericht, en voor het decoderen van de gecodeerde vijfde hash met de publieke sleutel van de ontvangcomputer voor het verifiëren van de digitale ondertekening van het antwoord EDI bevestigingsbericht; en middelen voor het berekenen van een zesde hash van het ontvangen antwoord EDI bevestigingsbericht; en middelen voor het vergelijken van de zesde hash met de gedecodeerde vijfde hash, waarbij de vergelijkingsmiddelen middelen bevatten voor het verschaffen van een indicatie van integriteit van het ontvangen antwoord EDI bevestigingsbericht en niet-afwijzing van oorsprong van het antwoord EDI bevestigingsbericht; waardoor niet-afwijzing van ontvangst van de EDI uitwisselingscommunicatie tot stand gebracht wordt door de zendcomputer.

6. Een verbeterd veilig open netwerkcommunicatiesysteem volgens conclusie 5, waarin de middelen voor het opwekken van het antwoord EDI bevestigingsbericht verder middelen bevatten voor het invoegen van de vierde hash in een vooraf bepaalde plaats in het verzonden antwoord EDI bevestigingsbericht en waarbij de middelen geassocieerd met de zendcomputer verder middelen bevatten voor het vergelijken van de vierde hash in het ontvangen antwoord EDI bevestigingsbericht met de eerste hash, waarbij de vergelijkingsmiddelen een indicatie van integriteit en authenticiteit van de EDI uitwisseling verschaffen wanneer de eerste en vierde hash met elkaar overeenkomen.

7. Een verbeterd veilig open netwerkcommunicatiesysteem volgens conclusie 6, waarin het EDI bevestigingsbericht een AUTACK bericht bevatten.

8. Een verbeterd veilig open netwerkcommunicatiesysteem volgens conclusie 7, waarin het antwoord EDI bevestigingsbericht een AUTACK bericht bevat.

9. Een verbeterd veilig open netwerkcommunicatiesysteem volgens conclusie 8, waarin elk van de hashes een MD5 bevat.

10. Een verbeterd veilig open netwerkcommunicatiesysteem volgens conclusie 9, waarin de publieke en privé sleutels een RSA type cryptografisch communicatiesysteem bevatten.

11. Een verbeterd veilig open netwerkcommunicatiesysteem volgens conclusie 10, waarin het open publieke netwerk het Internet bevat.

12. Een verbeterd veilig open netwerkcommunicatiesysteem volgens conclusie 1, waarin het open netwerk het Internet bevat.

13. Een verbeterd veilig open netwerkcommunicatiesysteem volgens conclusie 1, waarin de middelen geassocieerd met de ontvangcomputer verder middelen bevatten voor het opwekken van een antwoord EDI bevestigingsbericht en het verzenden van het antwoord EDI bevestigingsbericht naar de zendcomputer over het open publieke netwerk, waarbij de

middelen voor het opwekken van het antwoord EDI bevestigingsbericht middelen bevatten voor het berekenen van een derde hash van het antwoord EDI bevestigingsbericht en voor het digitaal ondertekenen van de derde hash door het coderen van de derde hash met de privé sleutel van de ontvangcomputer; en middelen voor het invoegen van de digitaal ondertekende derde hash in een vooraf bepaalde plaats in het verzonden antwoord EDI bevestigingsbericht.

14. Een verbeterd veilig open netwerkcommunicatiesysteem volgens conclusie 13, waarin het open publieke netwerk het Internet bevat.

15. Een verbeterd veilig open netwerkcommunicatiesysteem volgens conclusie 14, verder bevattende middelen geassocieerd met de zendcomputer voor het ontvangen van het verzonden antwoord EDI bevestigingsbericht, en voor het decoderen van de gecodeerde derde hash met de publieke sleutel van de ontvangcomputer voor het verifiëren van de digitale ondertekening van het antwoord EDI bevestigingsbericht; en middelen voor het berekenen van een vierde hash van het ontvangen antwoord EDI bevestigingsbericht; en middelen voor het vergelijken van de vierde hash met de gedecodeerde derde hash, waarbij de vergelijkingsmiddelen middelen bevatten voor het verschaffen van een indicatie van integriteit van het ontvangen antwoord EDI bevestigingsbericht en niet-afwijzing van oorsprong van het antwoord EDI bevestigingsbericht; waardoor niet-afwijzing van ontvangst van de EDI uitwisselingscommunicatie tot stand gebracht wordt door de zendcomputer.

16. Een verbeterd veilig open netwerkcommunicatiesysteem volgens conclusie 13, verder bevattende middelen geassocieerd met de zendcomputer voor het ontvangen van het verzonden antwoord EDI bevestigingsbericht, en voor het decoderen van de gecodeerde derde hash met de publieke sleutel van de ontvangcomputer voor het verifiëren van de digitale ondertekening van het antwoord EDI bevestigingsbericht; en middelen voor het berekenen van een vierde hash van het ontvangen antwoord antwoord EDI bevestigingsbe-

richt; en middelen voor het vergelijken van de vierde hash met de gedecodeerde derde hash, waarbij de vergelijkingsmiddelen middelen bevatten voor het verschaffen van een indicatie van integriteit van het ontvangen antwoord EDI bevestigingsbericht en niet-afwijzing van oorsprong van het antwoord EDI bevestigingsbericht; waardoor niet-afwijzing van ontvangst van de EDI uitwisselingscommunicatie tot stand gebracht wordt door de zendcomputer.

17. Een verbeterd veilig open netwerkcommunicatiesysteem volgens conclusie 4, waarin de middelen voor het opwekken van het antwoord EDI bevestigingsbericht verder middelen bevatten voor het invoegen van de vierde hash in een vooraf bepaalde plaats in het verzonden antwoord EDI bevestigingsbericht, en waarbij de middelen geassocieerd met de zendcomputer verder middelen bevatten voor het vergelijken van de vierde hash in het ontvangen antwoord EDI bevestigingsbericht met de eerste hash, waarbij de vergelijkingsmiddelen een indicatie van integriteit en authenticiteit van de EDI uitwisseling verschaffen wanneer de eerste en vierde hash met elkaar overeenkomen.

18. Een verbeterd veilig open netwerkcommunicatiesysteem volgens conclusie 1, waarin het EDI bevestigingsbericht een AUTACK bericht bevat.

19. Een verbeterd veilig open netwerkcommunicatiesysteem volgens conclusie 18, waarin het open publieke netwerk het Internet bevat.

20. Een verbeterd veilig open netwerkcommunicatiesysteem volgens conclusie 19, waarin elk van de hashes een MD5 bevat.

21. Een verbeterd veilig open netwerkcommunicatiesysteem volgens conclusie 1, waarin elk van de hashes een MD5 bevat.

22. Een verbeterd veilig open netwerkcommunicatiesysteem volgens conclusie 21, waarin het open publieke netwerk het Internet bevat.

23. Een verbeterd veilig open netwerkcommunicatiesysteem volgens conclusie 21, waarin het EDI bevestigingsbericht een AUTACK bericht bevat.

24. Een verbeterd veilig open netwerkcommunicatiesysteem volgens conclusie 23, waarin de publieke en privé sleutels een RSA type cryptografisch communicatiesysteem bevatten.

25. Een verbeterd veilig open netwerkcommunicatiesysteem volgens conclusie 24, waarin het open publieke netwerk het Internet bevat.

26. Een verbeterd veilig open netwerkcommunicatiesysteem volgens conclusie 1, waarin de publieke en privé sleutels een RSA type cryptografisch communicatiesysteem bevatten.

27. Een verbeterd veilig open netwerkcommunicatiesysteem volgens conclusie 26, waarin het open publieke netwerk het Internet bevat.

28. Een verbeterd veilig open netwerkcommunicatiesysteem volgens conclusie 13, waarin het EDI bevestigingsbericht een AUTACK bericht bevat.

29. Een verbeterd veilig open netwerkcommunicatiesysteem volgens conclusie 28, waarin het antwoord EDI bevestigingsbericht een AUTACK bericht bevat.

30. Een verbeterd veilig open netwerkcommunicatiesysteem volgens conclusie 13, waarin het antwoord EDI bevestigingsbericht een AUTACK bericht bevat.

31. Een verbeterd veilig open netwerkcommunicatiesysteem volgens conclusie 1, verder bevattende middelen voor het opwekken van een handelspartner overeenkomst communicatie tussen de zendcomputer en de ontvangcomputer, waarbij de zendcomputer en de ontvangcomputer handelspartners bevatten, waarbij de handelspartner overeenkomst communicatie de publieke sleutels bevat in de EDI uitwisselingscommunicatie voor het mogelijk maken dat de handelspartners certificatie aan elkaar verschaffen.

32. Een verbeterd veilig open netwerkcommunicatiesysteem volgens conclusie 31, waarin het open publieke netwerk het Internet bevat.

33. Een verbeterd veilig open netwerkcommunicatiesysteem volgens conclusie 32, waarin het EDI bevestigingsbericht een AUTACK bericht bevat.

34. Een verbeterd veilig open netwerkcommunicatiesysteem volgens conclusie 31, waarin het EDI bevestigingsbericht een AUTACK bericht bevat.

35. Een werkwijze voor het selectief verbinden van een groot aantal computers volgens een open publiek netwerk voor het verschaffen van een computer uitwisseling van privé veilige digitale berichten tussen een zendcomputer en een ontvangcomputer in het grote aantal computers, waarbij de zendcomputer een eerste geassocieerde publieke sleutel en een eerste geassocieerde privé sleutel heeft, waarbij de ontvangcomputer een tweede geassocieerde publieke sleutel en een tweede geassocieerde privé sleutel heeft, waarbij de digitale berichten een EDI uitwisselingscommunicatie bevatten tussen de zendcomputer en de ontvangcomputer, waarbij de EDI uitwisselingscommunicatie een geassocieerd EDI bevestigingsbericht heeft, waarbij de werkwijze de stappen bevat van het digitaal ondertekenen van het geassocieerde EDI bevestigingsbericht met de privé sleutel van de zendcomputer; het verzenden van de EDI uitwisselingscommunicatie samen met het digitaal ondertekende geassocieerde EDI bevestigingsbericht naar de ontvangcomputer over het open publieke netwerk; en het verwerken van het ontvangen digitaal ondertekende EDI bevestigingsbericht voor het verschaffen van authenticatie en niet-afwijzing van de EDI uitwisselingscommunicatie van de zendcomputer, waarbij de verwerkingsstap de stap bevat van het verwerken van het ontvangen digitaal ondertekende geassocieerde EDI bevestigingsbericht met de publieke sleutel van de zender; waardoor veilige privé EDI uitwisselingscommunicaties kunnen optreden over een open publiek netwerk onder het verschaffen van authenticatie van niet-afwijzing van de EDI commu-

nicatie onder gebruikmaking van het geassocieerde EDI bevestigingsbericht.

36. Een werkwijze voor het verschaffen van veilige privé communicaties over een open publiek netwerk volgens conclusie 35, waarin het open publieke netwerk het Internet bevat.

37. Een werkwijze voor het verschaffen van veilige privé communicaties over een open publiek netwerk volgens conclusie 36, verder bevattende de stappen van het opwekken van een antwoord EDI bevestigingsbericht van de ontvangcomputer; het digitaal ondertekenen van het antwoord EDI bevestigingsbericht met de privé sleutel van de ontvangcomputer; het verzenden van het digitaal ondertekende antwoord EDI bevestigingsbericht naar de zendcomputer over het open publieke netwerk, waarbij de zendcomputer het digitaal ondertekende antwoord EDI bevestigingsbericht ontvangt; en het verwerken van het ontvangen digitaal getekende antwoord EDI bevestigingsbericht voor het verschaffen van niet-afwijzing van ontvangst van de EDI uitwisselingscommunicatie door de zendcomputer, waarbij de verwerkingsstap de stap bevat van het verwerken van het ontvangen digitaal ondertekende antwoord EDI bevestigingsbericht met de publieke sleutel van de ontvangcomputer, waardoor niet-afwijzing van ontvangst van de EDI uitwisselingscommunicatie tot stand gebracht wordt door de zendcomputer.

38. Een werkwijze voor het verschaffen van veilige privé communicaties over een open publiek netwerk volgens conclusie 35, verder bevattende de stappen van het opwekken van een antwoord EDI bevestigingsbericht van de ontvangcomputer; het digitaal ondertekenen van het antwoord EDI bevestigingsbericht met de privé sleutel van de ontvangcomputer; het verzenden van het digitaal ondertekende antwoord EDI bevestigingsbericht naar de zendcomputer over het open publieke netwerk, waarbij de zendcomputer het digitaal ondertekende antwoord EDI bevestigingsbericht ontvangt; en het verwerken van het ontvangen digitaal ondertekende antwoord EDI bevestigingsbericht voor het verschaffen van

niet-afwijzing van ontvangst van de EDI uitwisselingscommunicatie tussen de zendcomputer, waarbij de verwerkingsstap de stap bevat van het verwerken van het ontvangen digitaal ondertekende antwoord EDI bevestigingsbericht met de publieke sleutel van de ontvangcomputer; waardoor niet-afwijzing van ontvangst van de EDI uitwisselingscommunicatie tot stand gebracht wordt door de zendcomputer.

39. Een werkwijze voor het verschaffen van veilige privé communicaties over een open publiek netwerk volgens conclusie 38, waarin de verwerkingsstap verder de stap bevat van het verschaffen van niet-afwijzing van oorsprong bij de ontvangcomputer van het ontvangen EDI bevestigingsbericht.

40. Een werkwijze voor het verschaffen van veilige privé communicaties over een open publiek netwerk volgens conclusie 39, waarin het open publieke netwerk het Internet bevat.

41. Een werkwijze voor het verschaffen van veilige privé communicaties over een open publiek netwerk volgens conclusie 35, waarin de verwerkingsstap verder de stap bevat van het verschaffen van niet-afwijzing van oorsprong bij de ontvangcomputer van het ontvangen EDI bevestigingsbericht.

42. Een werkwijze voor het verschaffen van veilige privé communicaties over een open publiek netwerk volgens conclusie 35, waarin het EDI bevestigingsbericht een AUTACK bericht bevat.

43. Een werkwijze voor het verschaffen van veilige privé communicaties over een open publiek netwerk volgens conclusie 38, waarin het antwoord EDI bevestigingsbericht een AUTACK bericht bevat.

44. Een werkwijze voor het verschaffen van veilige privé communicaties over een open publiek netwerk volgens conclusie 43, waarin het EDI bevestigingsbericht een AUTACK bericht bevat.

45. Een werkwijze voor het verschaffen van veilige privé communicaties over een open publiek netwerk volgens

conclusie 35, waarin de publieke en privé sleutels een RSA type cryptografisch communicatiesysteem bevatten.

46. Een werkwijze voor het verschaffen van veilige privé communicaties over een open publiek netwerk volgens conclusie 45, waarin het open publieke netwerk het Internet bevat.

47. Een werkwijze voor het verschaffen van veilige privé communicaties over een open publiek netwerk volgens conclusie 45, waarin het EDI bevestigingsbericht een AUTACK bericht bevat.

48. Een werkwijze voor het verschaffen van veilige privé communicaties over een open publiek netwerk in overeenstemming met conclusie 47, verder bevattende de stappen van het opwekken van een antwoord EDI bevestigingsbericht van de ontvangcomputer; het digitaal ondertekenen van het antwoord EDI bevestigingsbericht met de privé sleutel van de ontvangcomputer; het verzenden van het digitaal ondertekende antwoord EDI bevestigingsbericht naar de zendcomputer over het publieke netwerk, waarbij de zendcomputer het digitaal ondertekende antwoord EDI bevestigingsbericht ontvangt; en het verwerken van het ontvangen digitaal ondertekende antwoord EDI bevestigingsbericht voor het verschaffen van niet-afwijzing van ontvangst van de EDI uitwisselingscommunicatie door de zendcomputer, waarbij de verwerkingsstap de stap bevat van het verwerken van het ontvangen digitaal ondertekende antwoord EDI bevestigingsbericht met de publieke sleutel van de ontvangcomputer; waardoor niet-afwijzing van ontvangst van de EDI uitwisselingscommunicatie tot stand gebracht wordt door de zendcomputer.

49. Een werkwijze voor het verschaffen van veilige privé communicaties over een open publiek netwerk volgens conclusie 48, waarin het antwoord EDI bevestigingsbericht een AUTACK bericht bevat.

50. Een werkwijze voor het verschaffen van veilige privé communicaties over een open publiek netwerk volgens

conclusie 49, waarin het open publieke netwerk het Internet bevat.

1003644

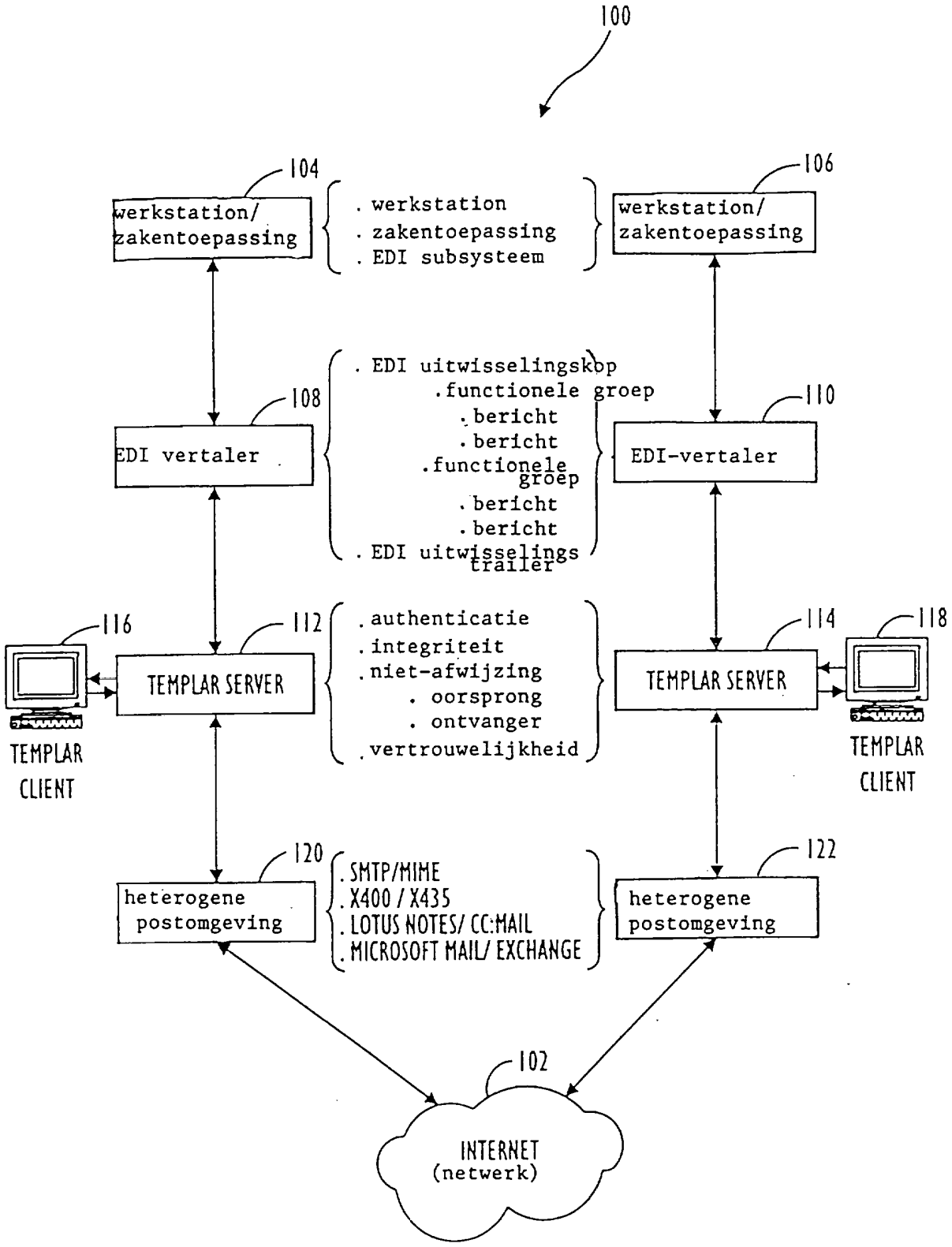

FIG. 1

1003644

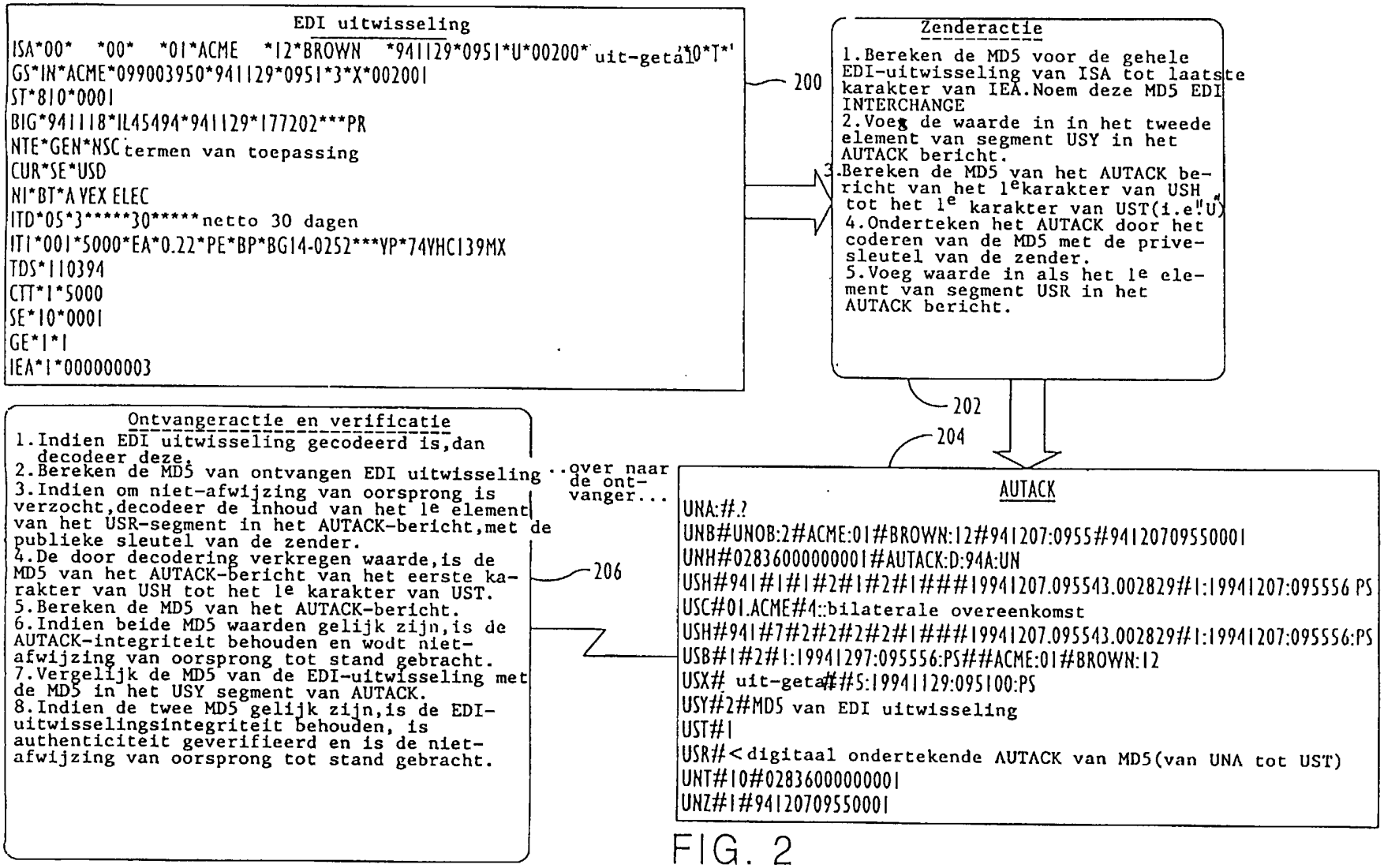
EDI uitwisseling
ISA*00* *00* *01*ACME *12*BROWN *941129*0951*U*00200* uit-geta10*T*'
GS*IN*ACME*099003950*941129*0951*3*X*002001
ST*810*0001
BIG*941118*IL45494*941129*177202***PR
NTE*GEN*NSC termen van toepassing
CUR*SE*USD
NI*BT*A YEX ELEC
ITD*05*3*****30*****netto 30 dagen
IT1*001*5000*EA*0.22*PE*BP*BG14-0252***YP*74YHC139MX
TDS*110394
CTT*1*5000
SE*10*0001
GE*1*1
IEA*1*000000003
200
Zenderactie
1.Bereken de MD5 voor de gehele EDI-uitwisseling van ISA tot laatste karakter van IEA.Noem deze MD5 EDI INTERCHANGE
2.Voeg de waarde in in het tweede element van segment USY in het AUTACK bericht.
3.Bereken de MD5 van het AUTACK bericht van het 1e karakter van USH tot het 1e karakter van UST(i.e."U")
4.Onderteken het AUTACK door het coderen van de MD5 met de privesleutel van de zender.
5.Voeg waarde in als het 1e element van segment USR in het AUTACK bericht.
202
204
Ontvangeractie en verificatie
1.Indien EDI uitwisseling gecodeerd is,dan decodeer deze.
2.Bereken de MD5 van ontvangen EDI uitwisseling
3.Indien om niet-afwijzing van oorsprong is verzocht,decodeer de inhoud van het 1e element van het USR-segment in het AUTACK-bericht,met de publieke sleutel van de zender.
4.De door decodering verkregen waarde,is de MD5 van het AUTACK-bericht van het eerste karakter van USH tot het 1e karakter van UST.
5.Bereken de MD5 van het AUTACK-bericht.
6.Indien beide MD5 waarden gelijk zijn,is de AUTACK-integriteit behouden en wodt niet-afwijzing van oorsprong tot stand gebracht.
7.Vergelijk de MD5 van de EDI-uitwisseling met de MD5 in het USY segment van AUTACK.
8.Indien de twee MD5 gelijk zijn,is de EDI-uitwisselingsintegriteit behouden, is authenticiteit geverifieerd en is de niet-afwijzing van oorsprong tot stand gebracht.
..over naar de ontvanger...
206
AUTACK
UNA:#.?
UNB#UNOB:2#ACME:01#BROWN:12#941207:0955#941207095500001
UNH#02836000000001#AUTACK:D:94A:UN
USH#941#1#1#2#1#2#1###19941207.095543.002829#1:19941207:095556 PS
USC#01.ACME#4::bilaterale overeenkomst
USH#941#7#2#2#2#2#1###19941207.095543.002829#1:19941207:095556:PS
USB#1#2#1:19941297:095556:PS##ACME:01#BROWN:12
USX# uit-geta##5:19941129:095100:PS
USY#2#MD5 van EDI uitwisseling
UST#1
USR#<digitaal ondertekende AUTACK van MD5(van UNA tot UST)
UNT#10#02836000000001
UNZ#1#941207095500001

FIG. 2

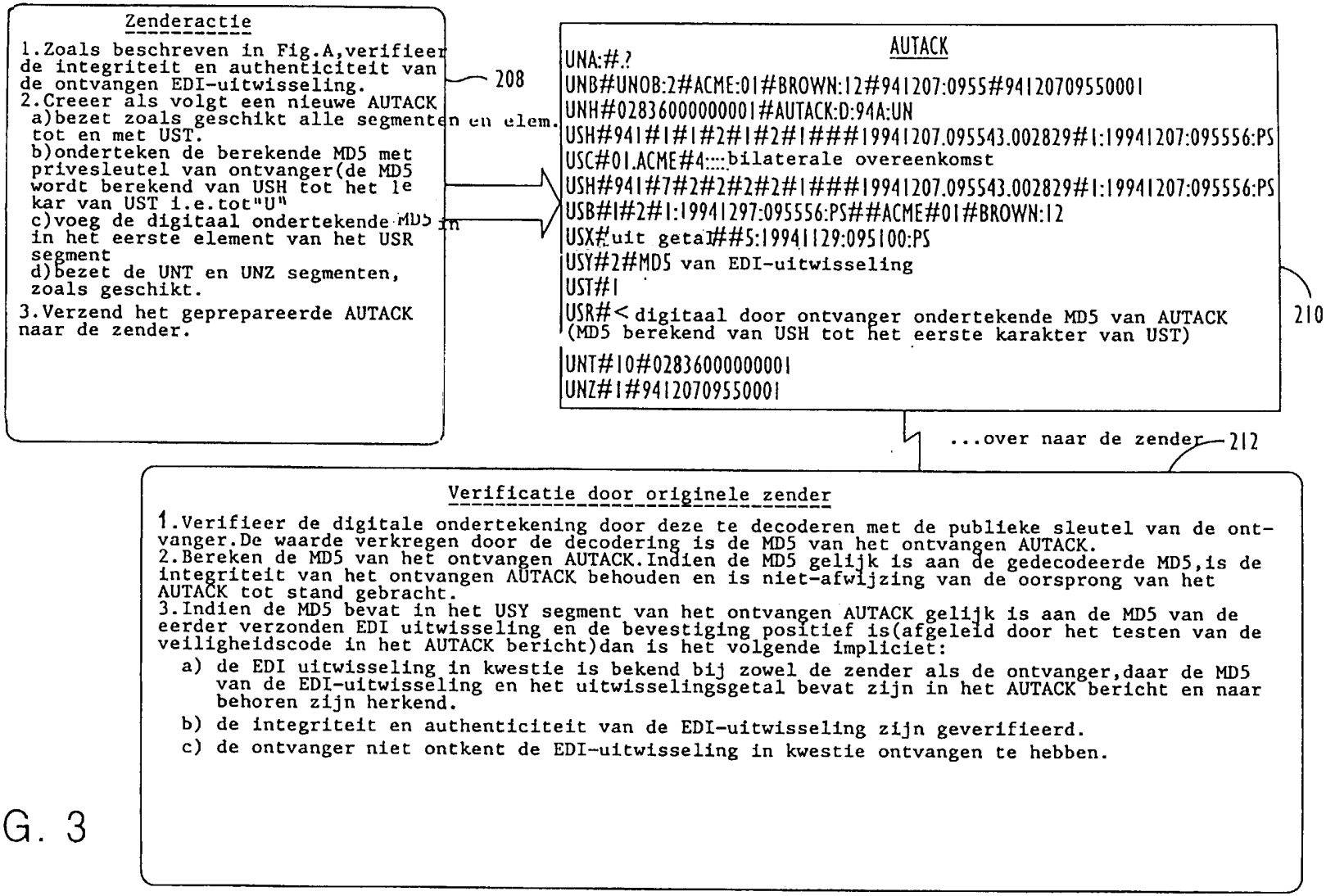
Zenderactie
1.Zoals beschreven in Fig.A,verifieer de integriteit en authenticiteit van de ontvangen EDI-uitwisseling.
2.Creeer als volgt een nieuwe AUTACK
a)bezet zoals geschikt alle segmenten en elem. tot en met UST.
b)onderteken de berekende MD5 met privesleutel van ontvanger(de MD5 wordt berekend van USH tot het 1e kar van UST i.e.tot"U"
c)voeg de digitaal ondertekende MD5 in in het eerste element van het USR segment
d)bezet de UNT en UNZ segmenten, zoals geschikt.
3.Verzend het geprepareerde AUTACK naar de zender.
208
AUTACK
UNA:#.?
UNB#UNOB:2#ACME:01#BROWN:12#941207:0955#94120709550001
UNH#02836000000001#AUTACK:D:94A:UN
USH#941#1#1#2#1#2#1###19941207.095543.002829#1:19941207:095556:PS
USC#01.ACME#4:::bilaterale overeenkomst
USH#941#7#2#2#2#2#1###19941207.095543.002829#1:19941207:095556:PS
USB#1#2#1:19941297:095556:PS##ACME#01#BROWN:12
USX#uit geta##5:19941129:095100:PS
USY#2#MD5 van EDI-uitwisseling
UST#1
USR#<digitaal door ontvanger ondertekende MD5 van AUTACK (MD5 berekend van USH tot het eerste karakter van UST)
UNT#10#02836000000001
UNZ#1#94120709550001
210
...over naar de zender
212
Verificatie door originele zender
1.Verifieer de digitale ondertekening door deze te decoderen met de publieke sleutel van de ontvanger.De waarde verkregen door de decodering is de MD5 van het ontvangen AUTACK.
2.Bereken de MD5 van het ontvangen AUTACK.Indien de MD5 gelijk is aan de gedecodeerde MD5,is de integriteit van het ontvangen AUTACK behouden en is niet-afwijzing van de oorsprong van het AUTACK tot stand gebracht.
3.Indien de MD5 bevat in het USY segment van het ontvangen AUTACK gelijk is aan de MD5 van de eerder verzonden EDI uitwisseling en de bevestiging positief is(afgeleid door het testen van de veiligheidscode in het AUTACK bericht)dan is het volgende impliciet:
a) de EDI uitwisseling in kwestie is bekend bij zowel de zender als de ontvanger,daar de MD5 van de EDI-uitwisseling en het uitwisselingsgetal bevat zijn in het AUTACK bericht en naar behoren zijn herkend.
b) de integriteit en authenticiteit van de EDI-uitwisseling zijn geverifieerd.
c) de ontvanger niet ontkent de EDI-uitwisseling in kwestie ontvangen te hebben.

FIG. 3

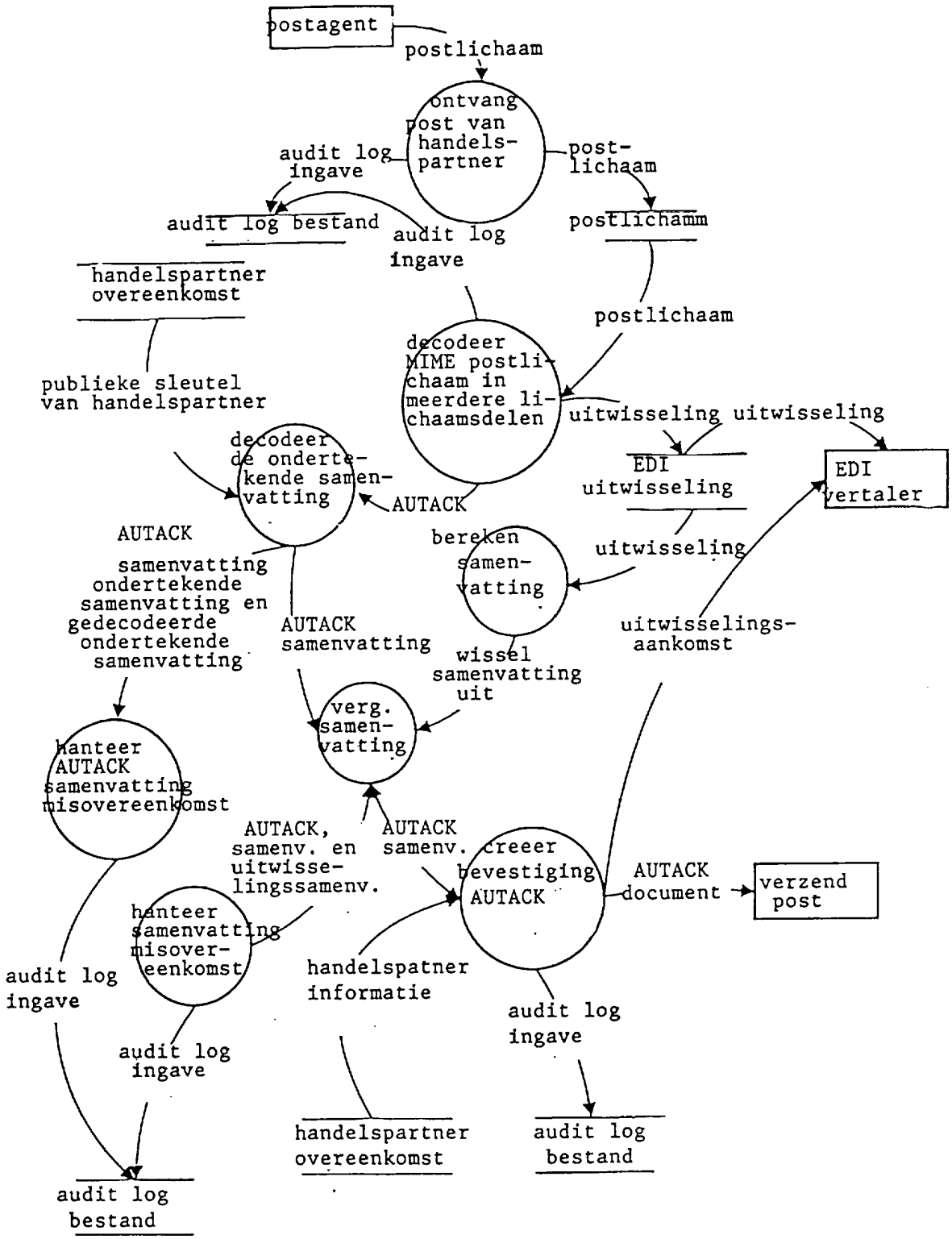
postagent
postlichaam
ontvang post van handels-partner
audit log ingave
post-lichaam
audit log bestand
audit log ingave
postlichamm
handelspartner overeenkomst
publieke sleutel van handelspartner
postlichaam
decodeer MIME postli-chaam in meerdere li-chaamsdelen
uitwisseling
uitwisseling
EDI uitwisseling
EDI vertaler
decodeer de onderte-kende samen-vatting
AUTACK
AUTACK samenvatting ondertekende samenvatting en gedecodeerde ondertekende samenvatting
bereken samen-vatting
uitwisseling
AUTACK samenvatting
wissel samenvatting uit
uitwisselings-aankomst
verg. samen-vatting
hanteer AUTACK samenvatting misovereenkomst
AUTACK, samenv. en uitwisse-lingssamenv.
AUTACK samenv.
creeer bevestiging AUTACK
AUTACK document
verzend post
hanteer samenvatting misover-eenkomst
audit log ingave
handelspatner informatie
audit log ingave
audit log ingave
handelspartner overeenkomst
audit log bestand
audit log bestand

FIG. 4

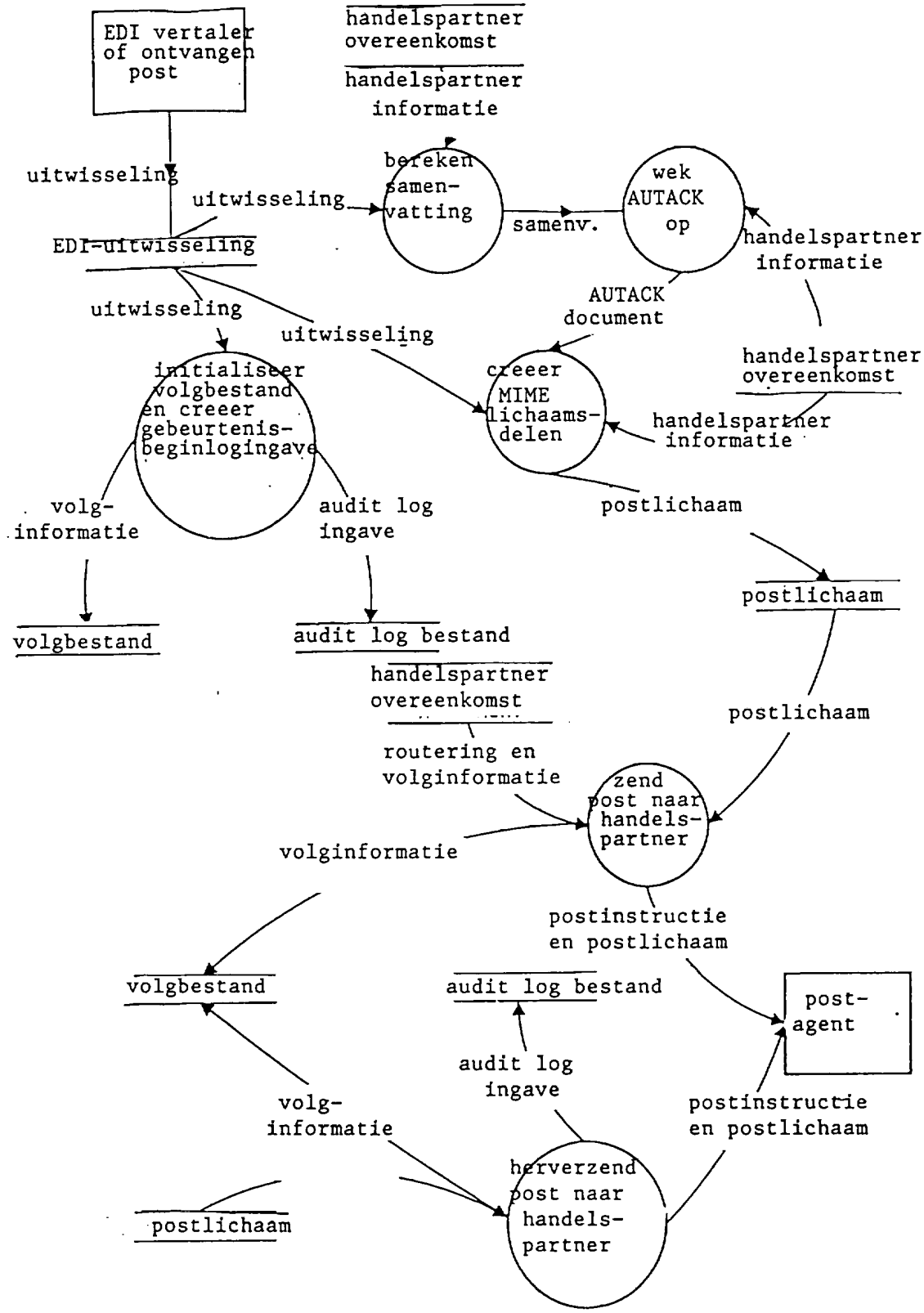
EDI vertaler of ontvangen post
handelspartner overeenkomst
handelspartner informatie
uitwisseling
uitwisseling
bereken samen-vatting
samenv.
wek AUTACK op
handelspartner informatie
EDI-uitwisseling
AUTACK document
uitwisseling
uitwisseling
initialiseer volgbestand en creeer gebeurtenis-beginlogingave
creeer MIME lichaams-delen
handelspartner overeenkomst
handelspartner informatie
volg-informatie
audit log ingave
postlichaam
postlichaam
volgbestand
audit log bestand
handelspartner overeenkomst
postlichaam
routering en volginformatie
zend post naar handels-partner
volginformatie
postinstructie en postlichaam
volgbestand
audit log bestand
post-agent
audit log ingave
volg-informatie
postinstructie en postlichaam
herverzend post naar handels-partner
postlichaam

FIG. 5

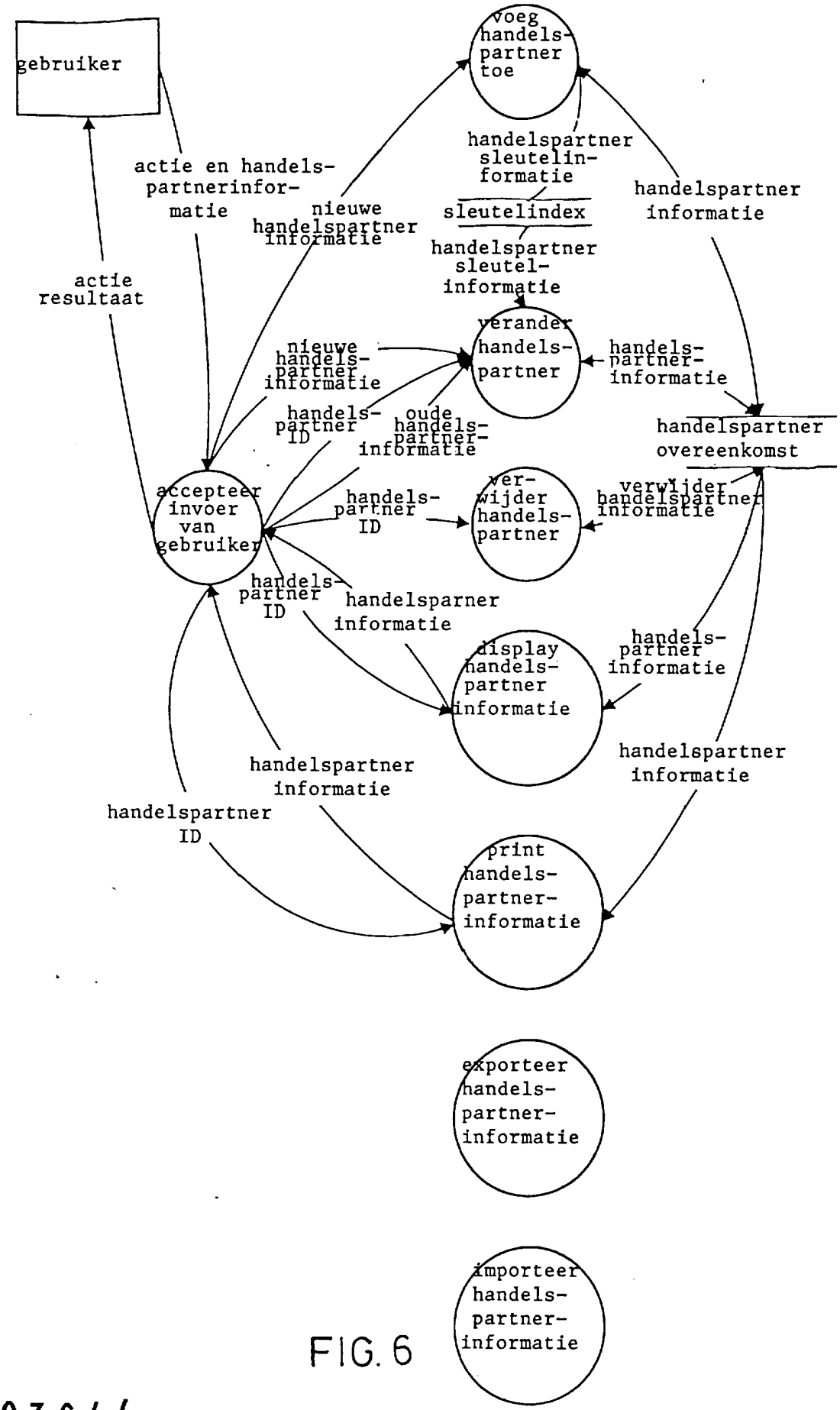
gebruiker
actie en handels-partnerinfor-matie
actie resultaat
voeg handels-partner toe
nieuwe handelspartner informatie
handelspartner sleutelin-formatie
sleutelindex
handelspartner sleutel-informatie
handelspartner informatie
verander handels-partner
nieuwe handels-partner informatie
handels-partner ID
oude handels-partner-informatie
handels-partner-informatie
handelspartner overeenkomst
accepteer invoer van gebruiker
handels-partner ID
ver-wijder handels-partner
verwijder handelspartner informatie
handels-partner ID
handelsparner informatie
display handels-partner informatie
handels-partner informatie
handelspartner informatie
handelspartner ID
handelspartner informatie
print handels-partner-informatie
exporteer handels-partner-informatie
importeer handels-partner-informatie

FIG. 6

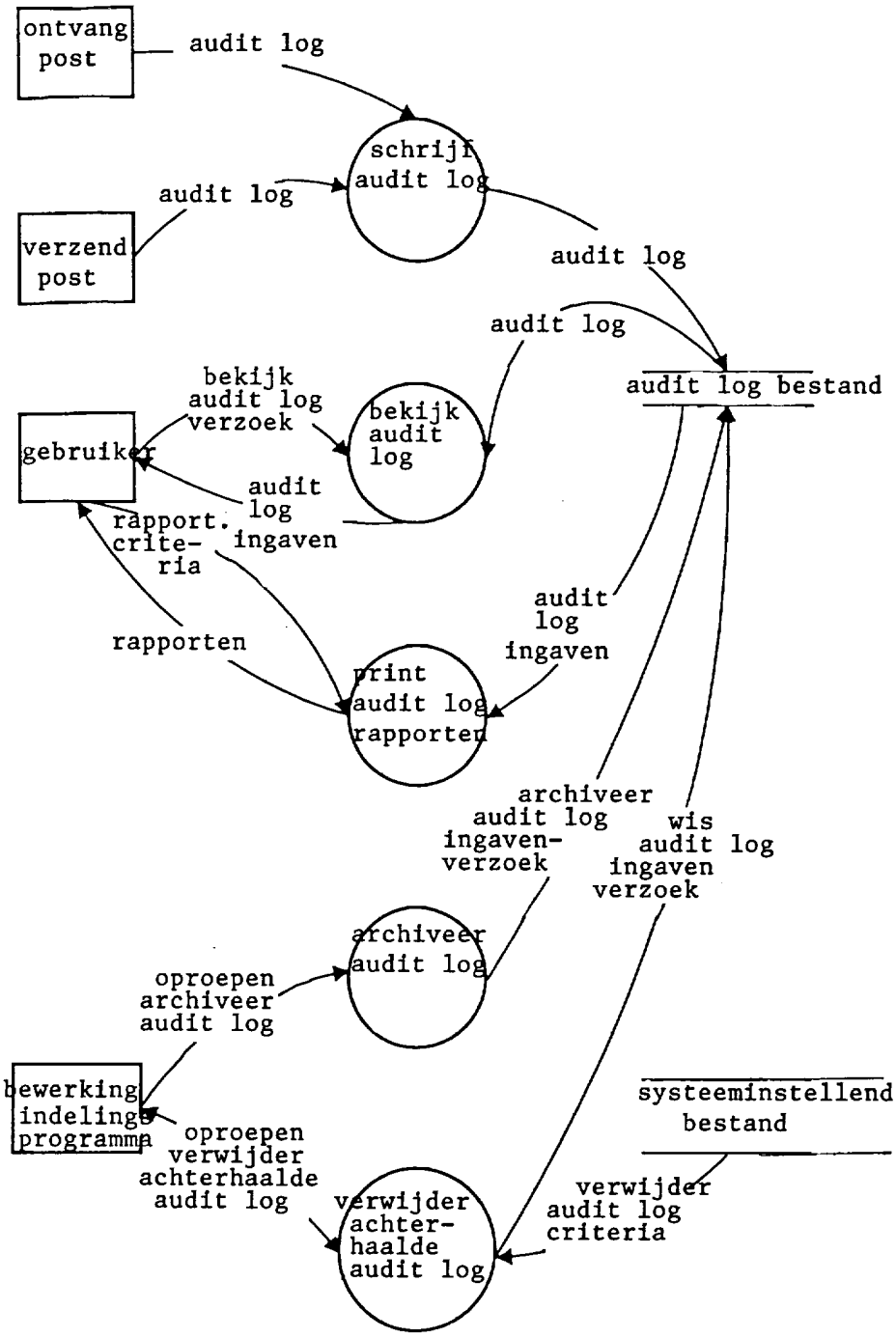
ontvang post
audit log
schrijf audit log
audit log
verzend post
audit log
audit log
audit log bestand
audit log
bekijk audit log verzoek
bekijk audit log
gebruiker
audit log
rapport. crite- ria
ingaven
audit log
ingaven
rapporten
print audit log rapporten
archiveer audit log
ingaven- verzoek
wis audit log ingaven verzoek
archiveer audit log
oproepen archiveer audit log
bewerking indelings programma
oproepen verwijder achterhaalde audit log
systeeminstellend bestand
verwijder audit log criteria
verwijder achter- haalde audit log

FIG.7

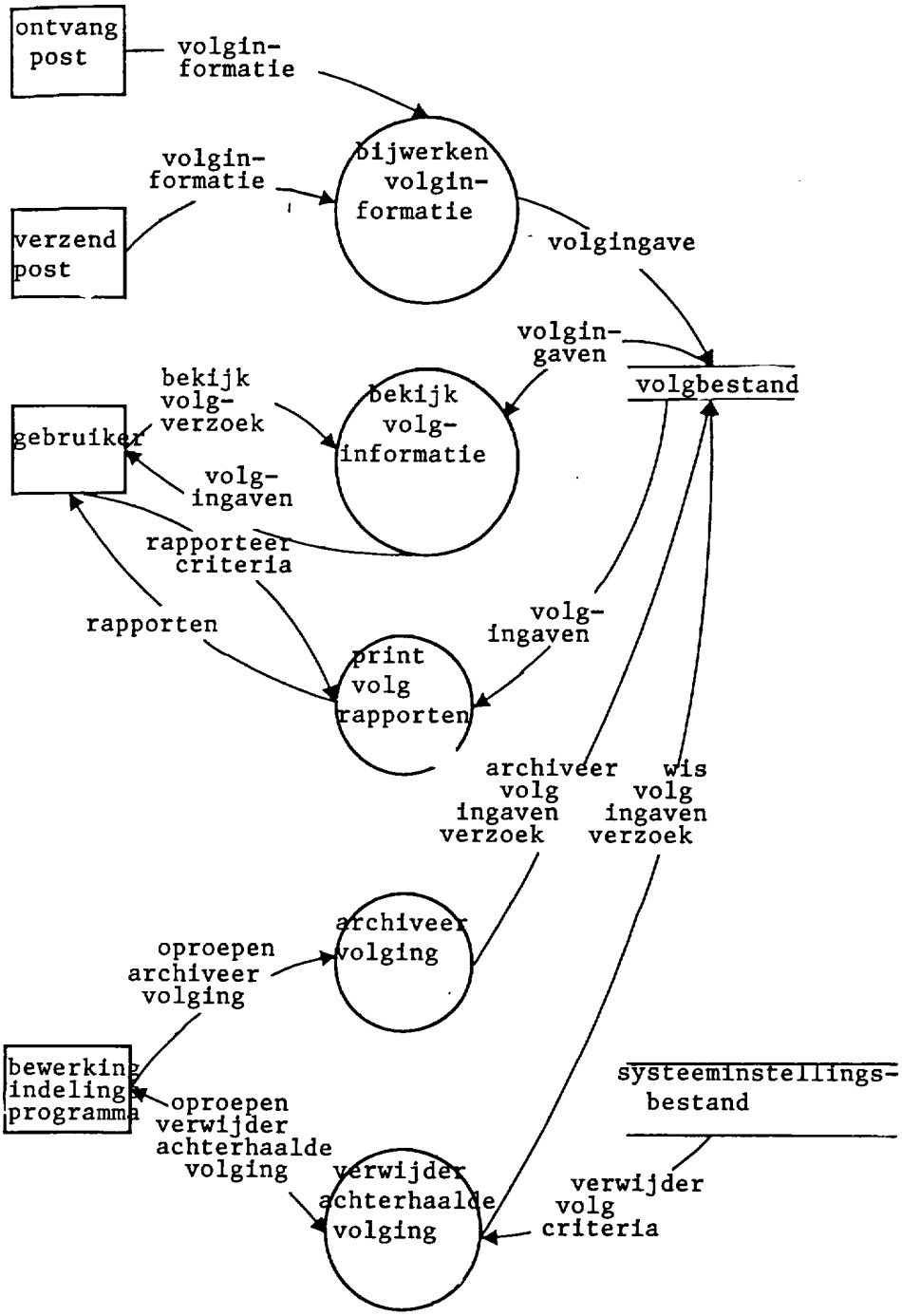
ontvang post
volgin-formatie
volgin-formatie
verzend post
bijwerken volgin-formatie
volgingave
volgin-gaven
volgbestand
bekijk volg-verzoek
gebruiker
bekijk volg-informatie
volg-ingaven
rapporteer criteria
rapporten
volg-ingaven
print volg rapporten
archiveer volg ingaven verzoek
wis volg ingaven verzoek
archiveer volging
oproepen archiveer volging
bewerking indeling programma
oproepen verwijder achterhaalde volging
systeeminstellings-bestand
verwijder achterhaalde volging
verwijder volg criteria

FIG.8

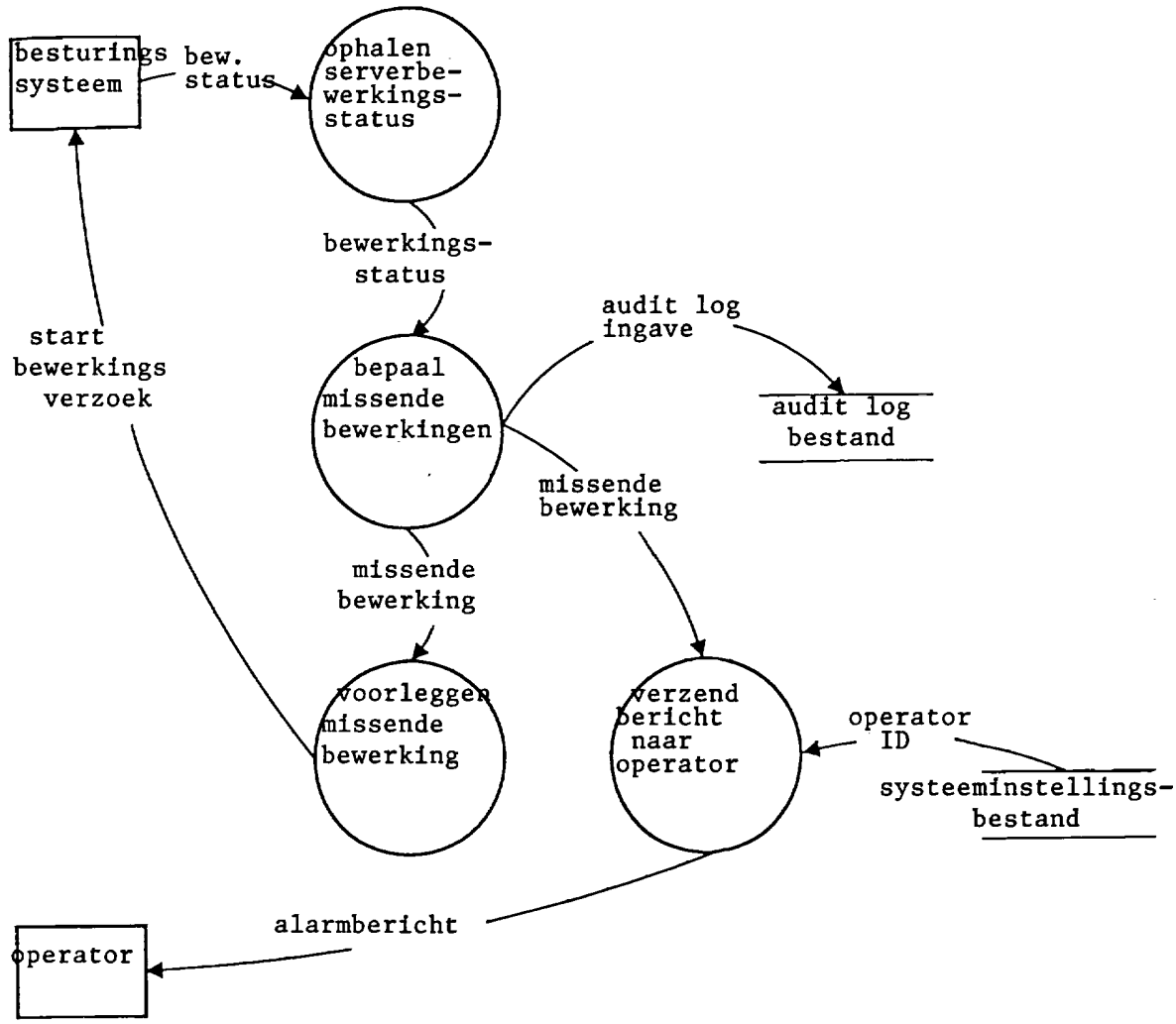
besturings systeem
bew. status
ophalen serverbe-werkings-status
bewerkings-status
audit log ingave
start bewerkings verzoek
bepaal missende bewerkingen
audit log bestand
missende bewerking
missende bewerking
voorleggen missende bewerking
verzend bericht naar operator
operator ID
systeeminstellings-bestand
alarmbericht
operator

FIG.9

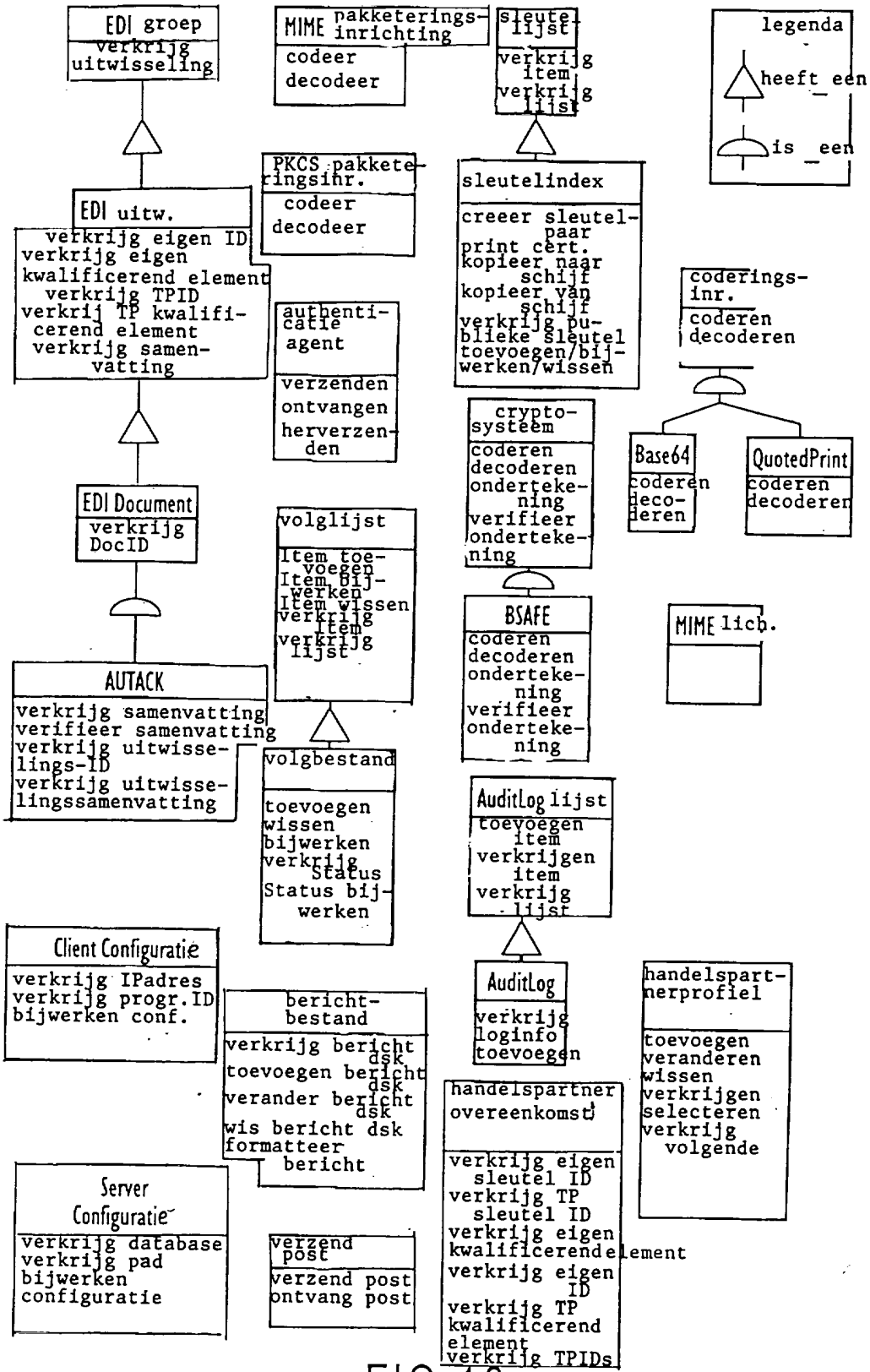
EDI groep
verkrijg uitwisseling
MIME pakketerings-inrichting
codeer
decodeer
sleutel lijst
verkrijg item
verkrijg lijst
legenda
heeft een
is een
EDI uitw.
verkrijg eigen ID
verkrijg eigen kwalificerend element
verkrijg TPID
verkrij TP kwalificerend element
verkrijg samenvatting
PKCS pakketeringsinr.
codeer
decodeer
sleutelindex
creeer sleutelpaar
print cert.
kopieer naar schijf
kopieer van schijf
verkrijg publieke sleutel
toevoegen/bijwerken/wissen
authenticatie agent
verzenden
ontvangen
herverzenden
coderingsinr.
coderen
decoderen
crypto-systeem
coderen
decoderen
ondertekening
verifieer ondertekening
Base64
coderen
decoderen
QuotedPrint
coderen
decoderen
EDI Document
verkrijg DocID
volglijst
Item toevoegen
Item bijwerken
Item wissen
verkrijg item
verkrijg lijst
BSAFE
coderen
decoderen
ondertekening
verifieer ondertekening
MIME lich.
AUTACK
verkrijg samenvatting
verifieer samenvatting
verkrijg uitwisselings-ID
verkrijg uitwisselingssamenvatting
volgbestand
toevoegen
wissen
bijwerken
verkrijg Status
Status bijwerken
AuditLog lijst
toevoegen item
verkrijgen item
verkrijg lijst
Client Configuratie
verkrijg IPadres
verkrijg progr.ID
bijwerken conf.
bericht-bestand
verkrijg bericht dsk
toevoegen bericht dsk
verander bericht dsk
wis bericht dsk
formatteer bericht
AuditLog
verkrijg loginfo
toevoegen
handelspartnerprofiel
toevoegen
veranderen
wissen
verkrijgen
selecteren
verkrijg volgende
handelspartner overeenkomst
verkrijg eigen sleutel ID
verkrijg TP sleutel ID
verkrijg eigen kwalificerend element
verkrijg eigen ID
verkrijg TP kwalificerend element
verkrijg TPIDs
Server Configuratie
verkrijg database
verkrijg pad
bijwerken configuratie
verzend post
verzend post
ontvang post

FIG.10

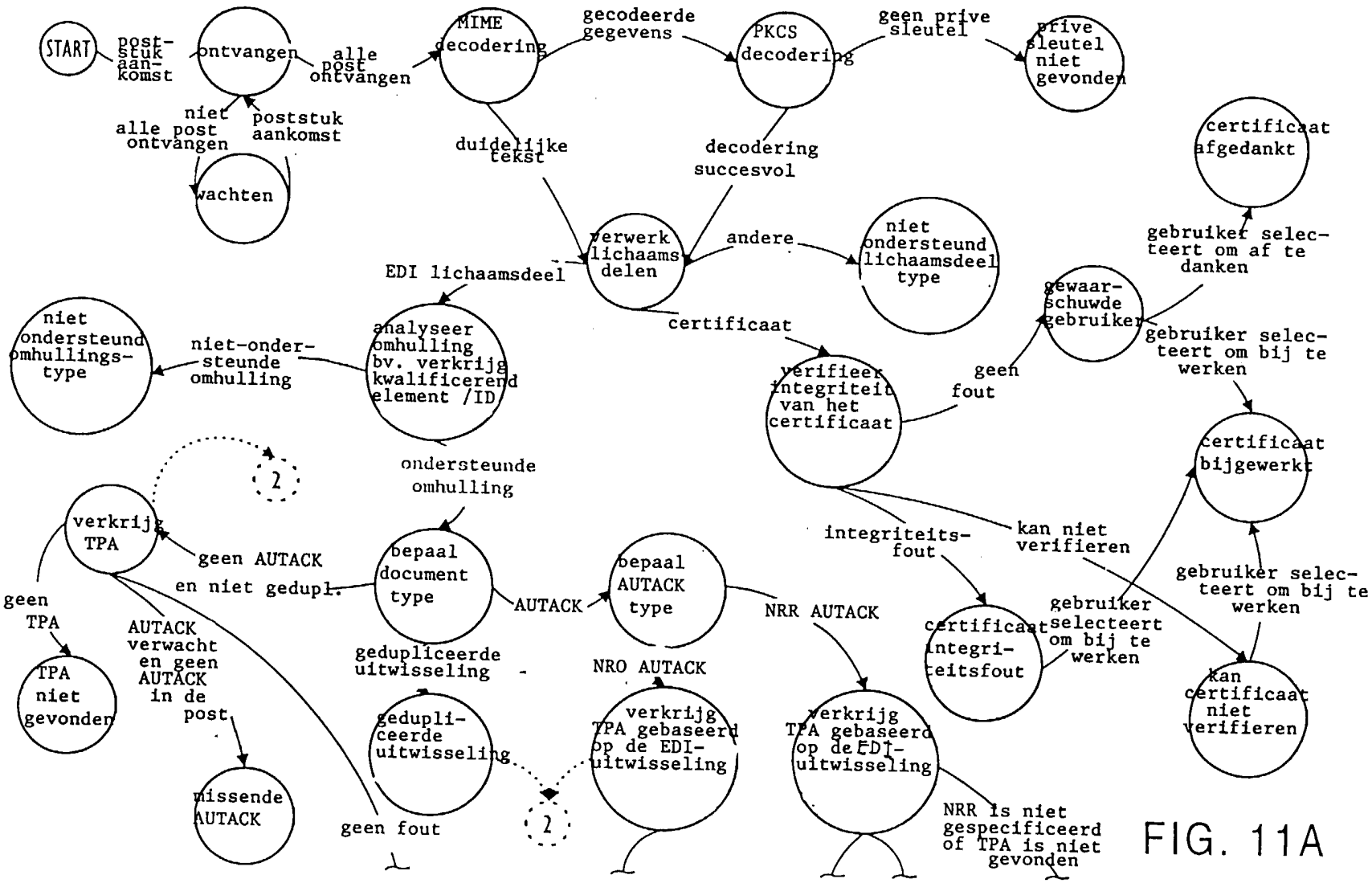
START
post-stuk aan-komst
ontvangen
alle post ontvangen
niet alle post ontvangen
poststuk aankomst
wachten
MIME decodering
gecodeerde gegevens
PKCS decodering
geen prive sleutel
prive sleutel niet gevonden
duidelijke tekst
decodering succesvol
verwerk lichaams delen
andere
niet ondersteund lichaamsdeel type
EDI lichaamsdeel
certificaat
certificaat afgedankt
gebruiker selecteert om af te danken
gewaar-schuwde gebruiker
gebruiker selecteert om bij te werken
verifieer integriteit van het certificaat
geen fout
niet ondersteund omhullings-type
niet-onder-steunde omhulling
analyseer omhulling bv. verkrijg kwalificerend element /ID
ondersteunde omhulling
certificaat bijgewerkt
integriteits-fout
kan niet verifieren
verkrijg TPA
geen AUTACK en niet gedupl.
bepaal document type
AUTACK
bepaal AUTACK type
NRR AUTACK
gebruiker selecteert om bij te werken
certificaat integri-teitsfout
kan certificaat niet verifieren
geen TPA
TPA niet gevonden
AUTACK verwacht en geen AUTACK in de post
gedupliceerde uitwisseling
NRO AUTACK
verkrijg TPA gebaseerd op de EDI-uitwisseling
verkrijg TPA gebaseerd op de EDI-uitwisseling
missende AUTACK
geen fout
NRR is niet gespecificeerd of TPA is niet gevonden
1
2
2

FIG. 11A

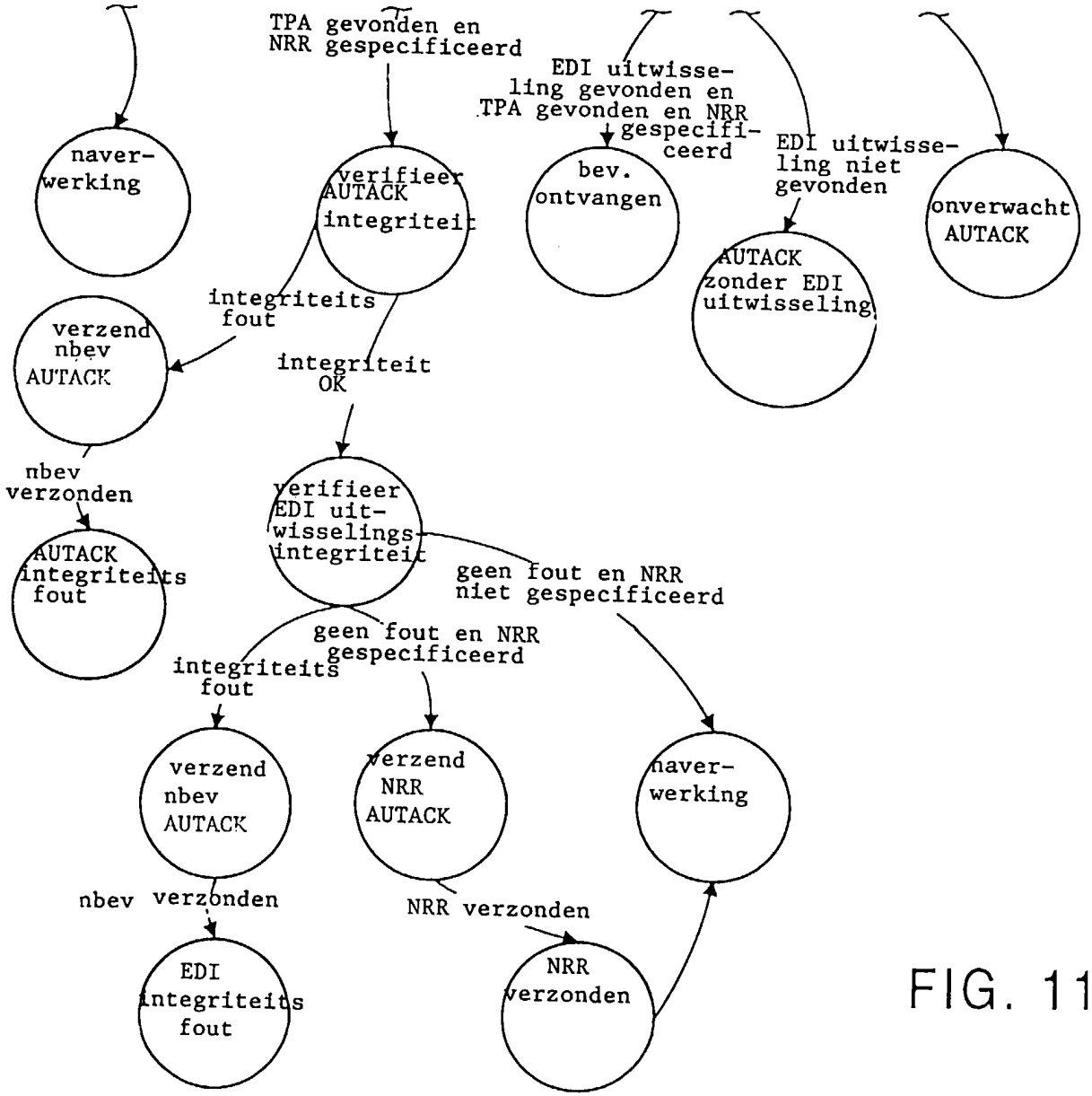
naver-
werking
TPA gevonden en
NRR gespecificeerd
verifieer
AUTACK
integriteit
EDI uitwisse-
ling gevonden en
TPA gevonden en NRR
gespecifi-
ceerd
bev.
ontvangen
EDI uitwisse-
ling niet
gevonden
AUTACK
zonder EDI
uitwisseling
onverwacht
AUTACK
integriteits
fout
verzend
nbev
AUTACK
integriteit
OK
nbev
verzonden
AUTACK
integriteits
fout
verifieer
EDI uit-
wisselings
integriteit
geen fout en NRR
niet gespecificeerd
geen fout en NRR
gespecificeerd
integriteits
fout
verzend
nbev
AUTACK
verzend
NRR
AUTACK
naver-
werking
nbev verzonden
NRR verzonden
EDI
integriteits
fout
NRR
verzonden

FIG. 11B

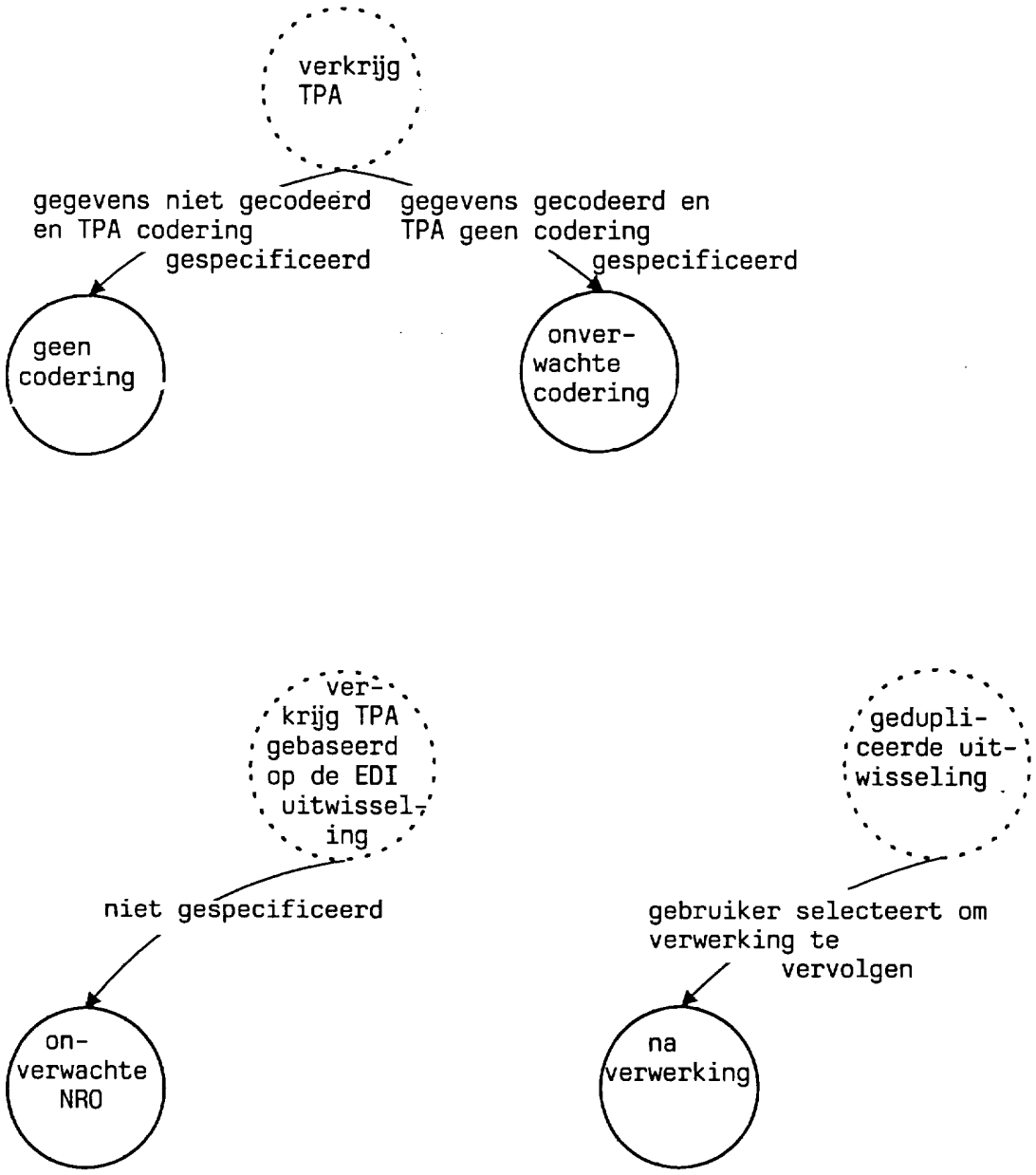
verkrijg TPA
gegevens niet gecodeerd en TPA codering gespecificeerd
gegevens gecodeerd en TPA geen codering gespecificeerd
geen codering
onver-wachte codering
ver-krijg TPA gebaseerd op de EDI uitwissel-ing
niet gespecificeerd
on-verwachte NRO
gedupli-ceerde uit-wisseling
gebruiker selecteert om verwerking te vervolgen
na verwerking

FIG. 12

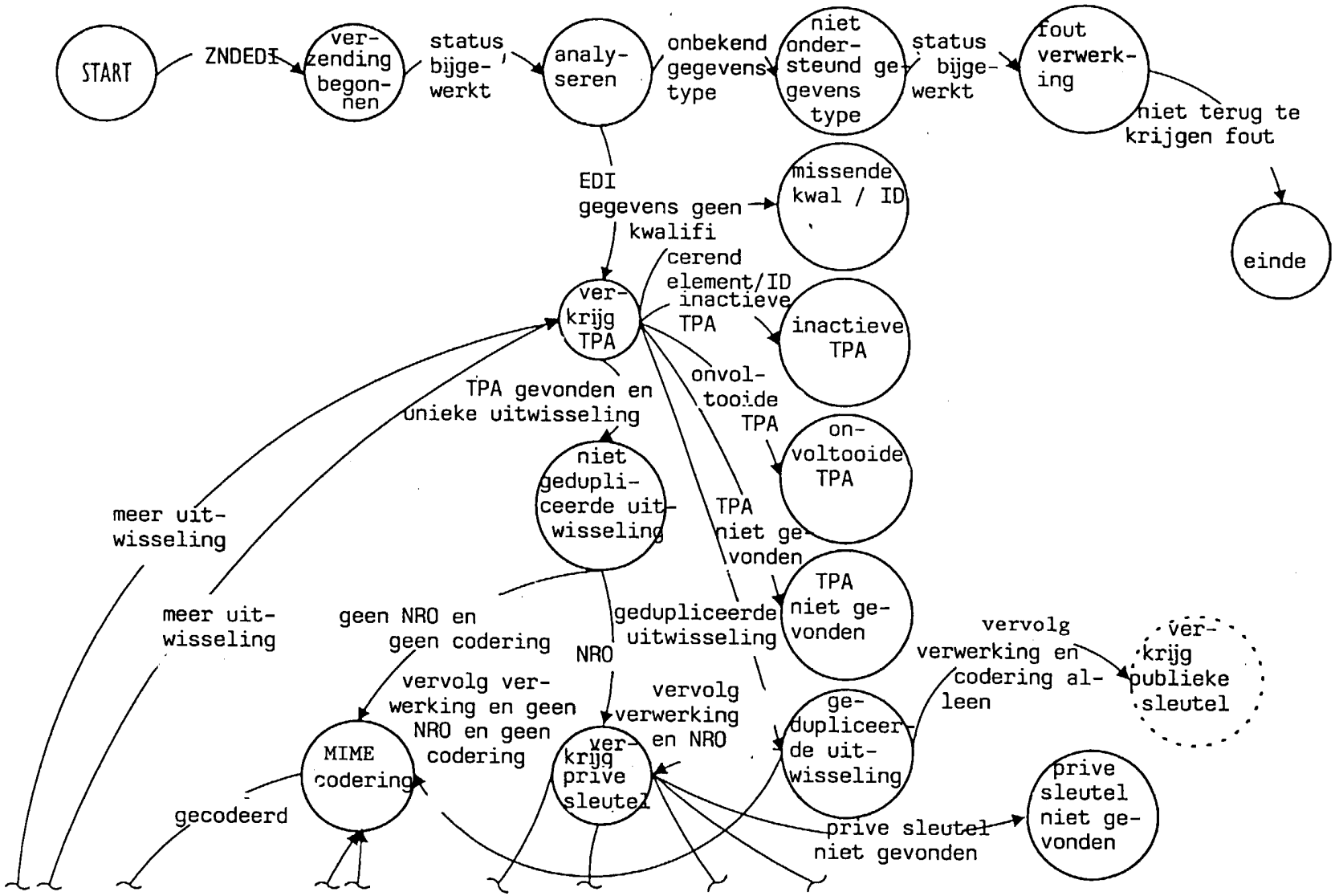
START
ZNDEDI
ver-zending begon-nen
status bijge-werkt
analy-seren
onbekend gegevens type
niet onder-steund ge-gevens type
status bijge-werkt
fout verwerk-ing
niet terug te krijgen fout
einde
EDI gegevens geen kwalifi
missende kwal / ID
cerend element/ID
ver-krijg TPA
inactieve TPA
inactieve TPA
onvol-tooide TPA
on-voltooide TPA
TPA gevonden en unieke uitwisseling
niet gedupli-ceerde uit-wisseling
TPA niet ge-vonden
TPA niet ge-vonden
meer uit-wisseling
meer uit-wisseling
geen NRO en geen codering
NRO
gedupliceerde uitwisseling
vervolg verwerking en codering al-leen
ver-krijg publieke sleutel
vervolg ver-werking en geen NRO en geen codering
vervolg verwerking en NRO
MIME codering
ver-krijg prive sleutel
ge-dupliceer-de uit-wisseling
gecodeerd
prive sleutel niet gevonden
prive sleutel niet ge-vonden

FIG. 13A

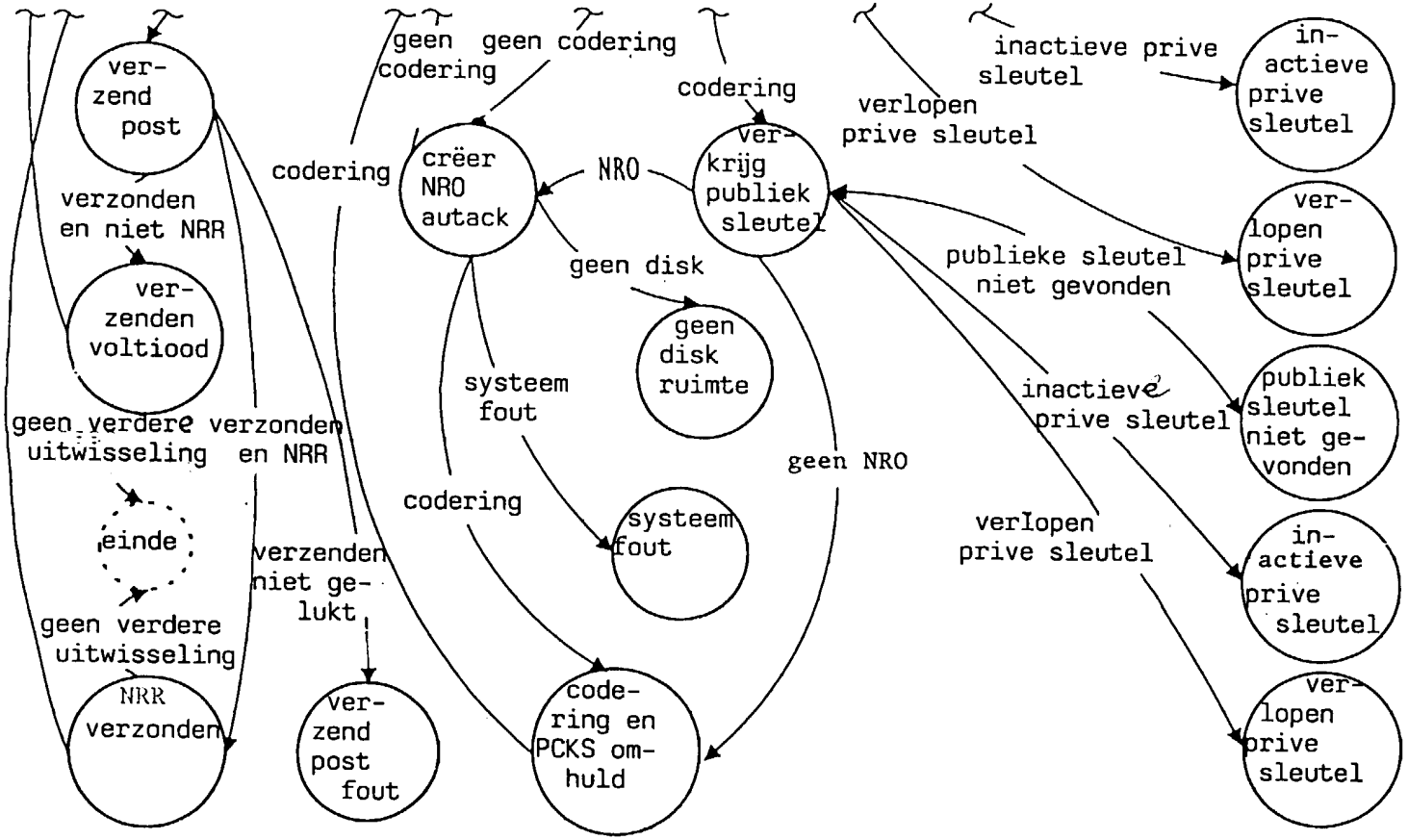
ver-
zend
post
verzonden
en niet NRR
ver-
zenden
voltiood
geen verdere
uitwisseling
einde
geen verdere
uitwisseling
NRR
verzonden
verzenden
en NRR
verzenden
niet ge-
lukt
ver-
zend
post
fout
codering
geen
codering
geen codering
creëer
NRO
autack
NRO
geen disk
systeem
fout
codering
systeem
fout
geen
disk
ruimte
codering
ver-
krijg
publiek
sleutel
geen NRO
code-
ring en
PCKS om-
huld
inactieve prive
sleutel
verlopen
prive sleutel
publieke sleutel
niet gevonden
inactieve
prive sleutel
verlopen
prive sleutel
in-
actieve
prive
sleutel
ver-
lopen
prive
sleutel
publiek
sleutel
niet ge-
vonden
in-
actieve
prive
sleutel
ver-
lopen
prive
sleutel

FIG. 13B

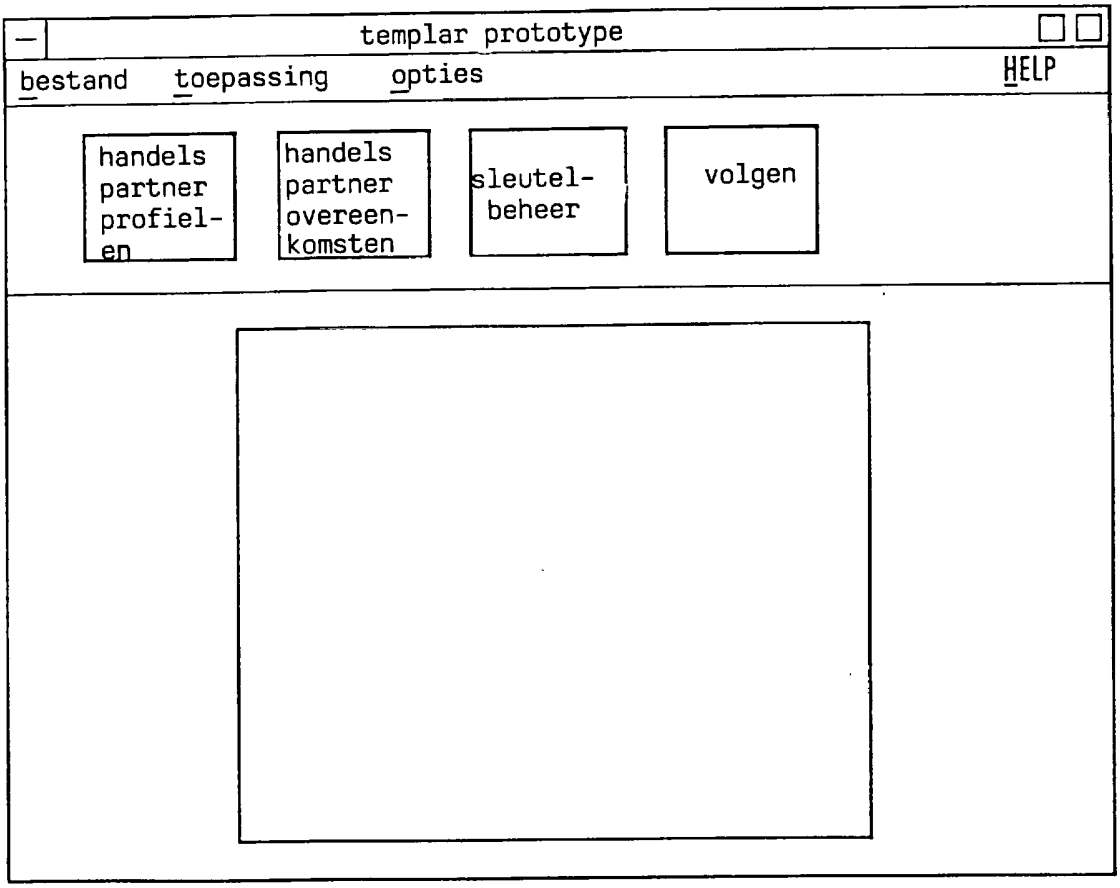
templar prototype
bestand
toepassing
opties
HELP
handels partner profiel-en
handels partner overeen-komsten
sleutel-beheer
volgen

FIG. 14

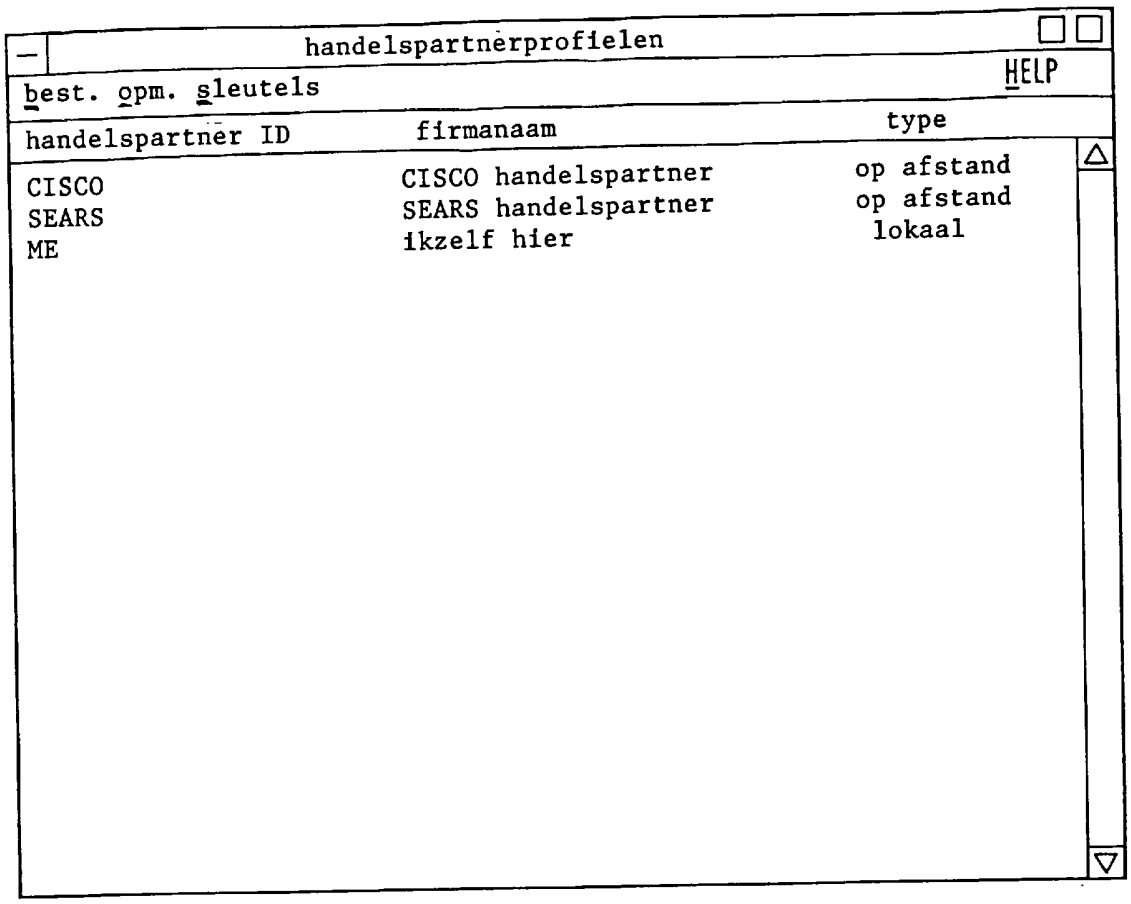
handelspartnerprofielen
HELP
best. opm. sleutels
handelspartner ID
firmanaam
type
CISCO
CISCO handelspartner
op afstand
SEARS
SEARS handelspartner
op afstand
ME
ikzelf hier
lokaal

FIG. 15

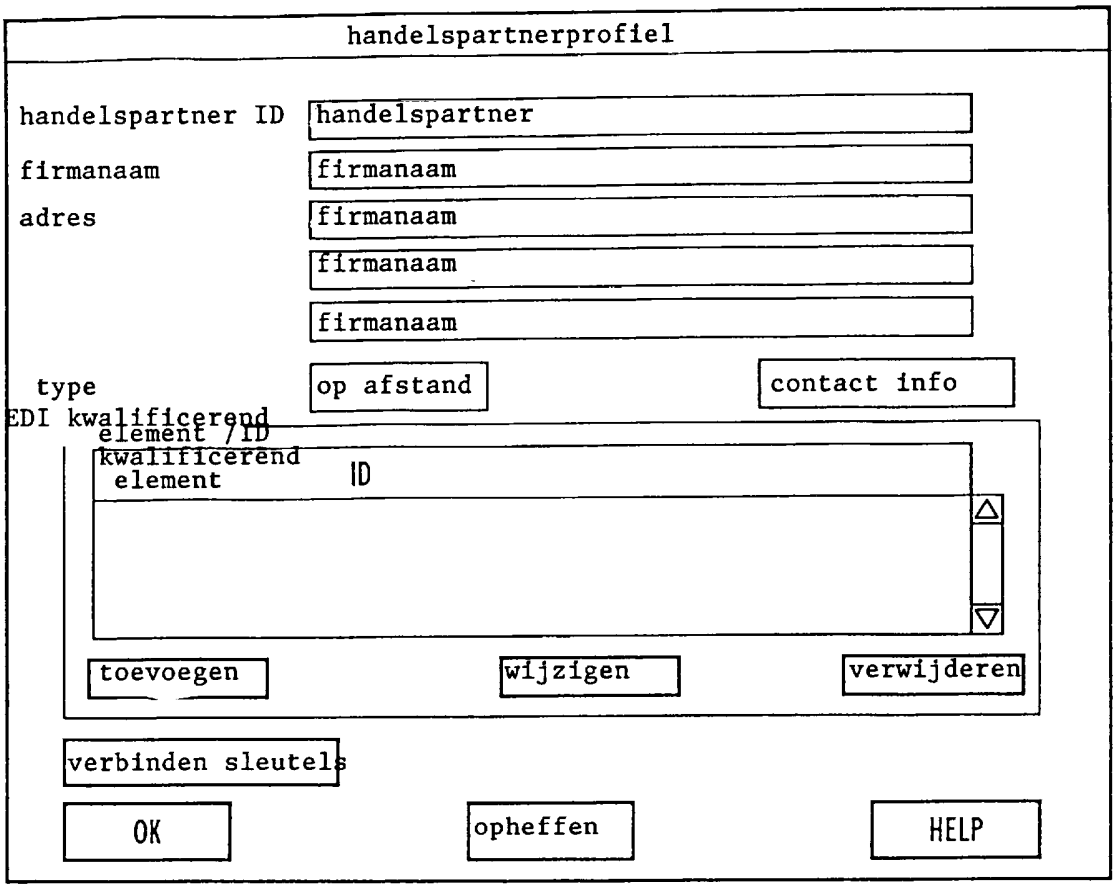
handelspartnerprofiel
handelspartner ID
handelspartner
firmanaam
firmanaam
adres
firmanaam
firmanaam
firmanaam
type
op afstand
contact info
EDI kwalificerend element /ID
kwalificerend element ID
toevoegen
wijzigen
verwijderen
verbinden sleutels
OK
opheffen
HELP

FIG. 16

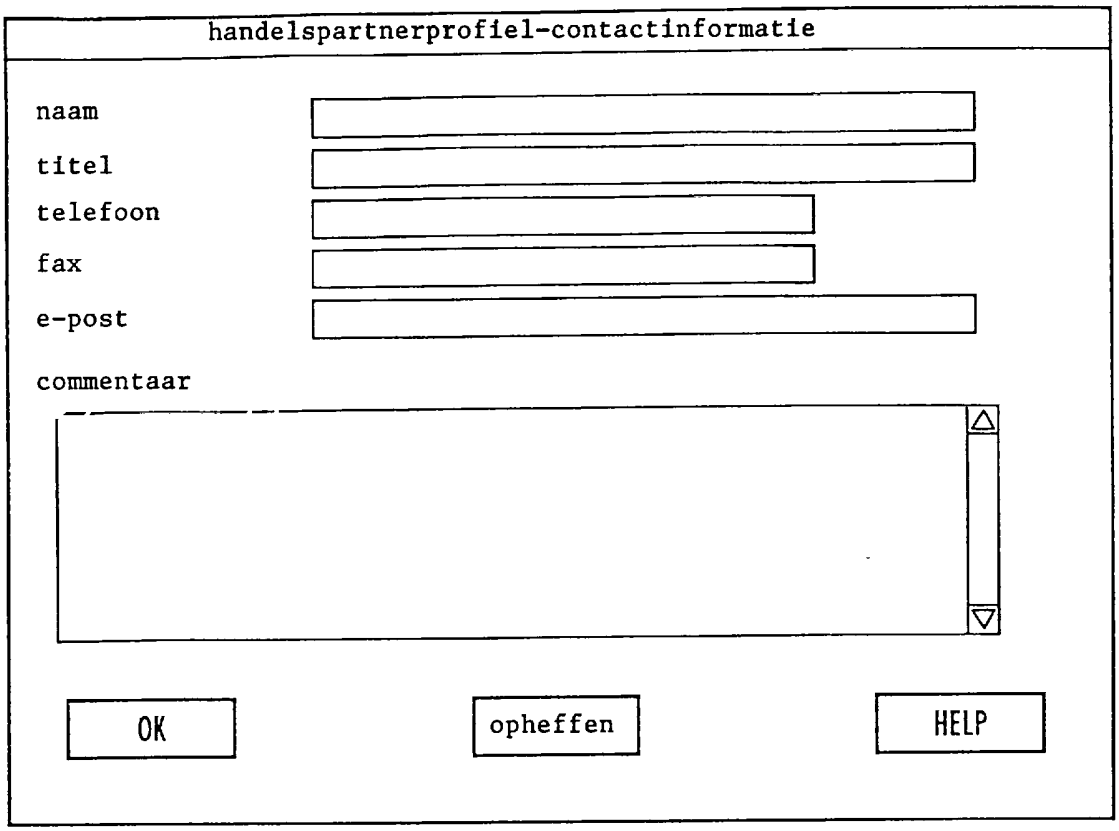
handelspartnerprofiel-contactinformatie
naam
titel
telefoon
fax
e-post
commentaar
OK
opheffen
HELP

FIG. 17

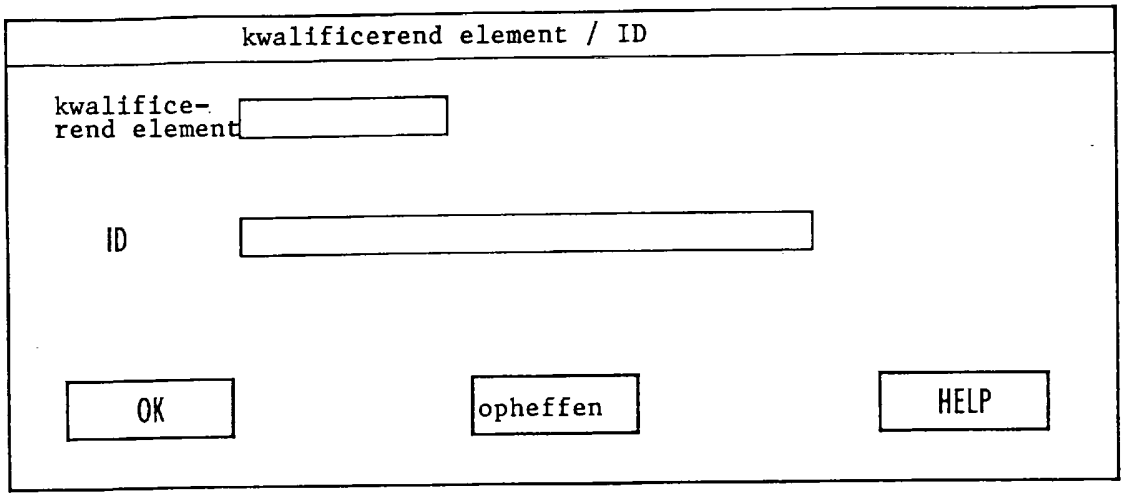
kwalificerend element / ID
kwalifice-
rend element
ID
OK
opheffen
HELP

FIG. 18

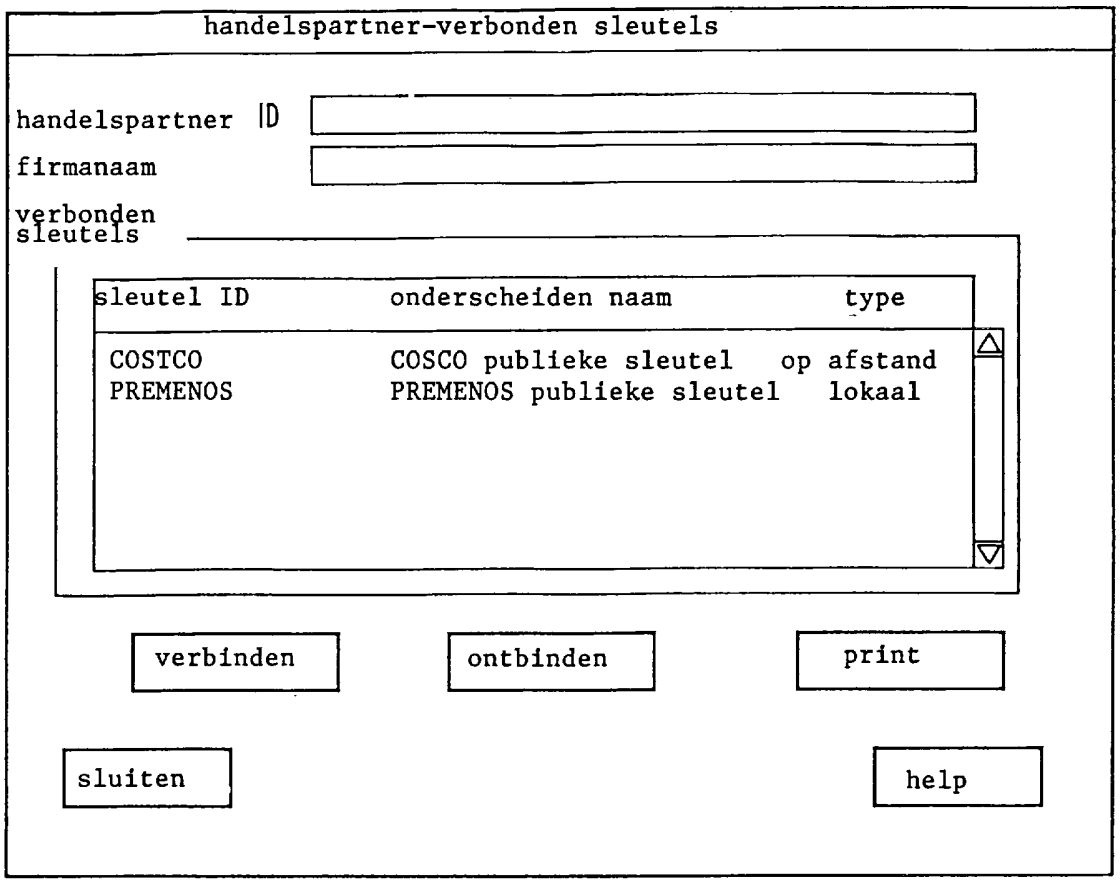
handelspartner-verbonden sleutels
handelspartner ID
firmanaam
verbonden sleutels
sleutel ID
onderscheiden naam
type
COSTCO
COSCO publieke sleutel
op afstand
PREMENOS
PREMENOS publieke sleutel
lokaal
verbinden
ontbinden
print
sluiten
help

FIG. 19

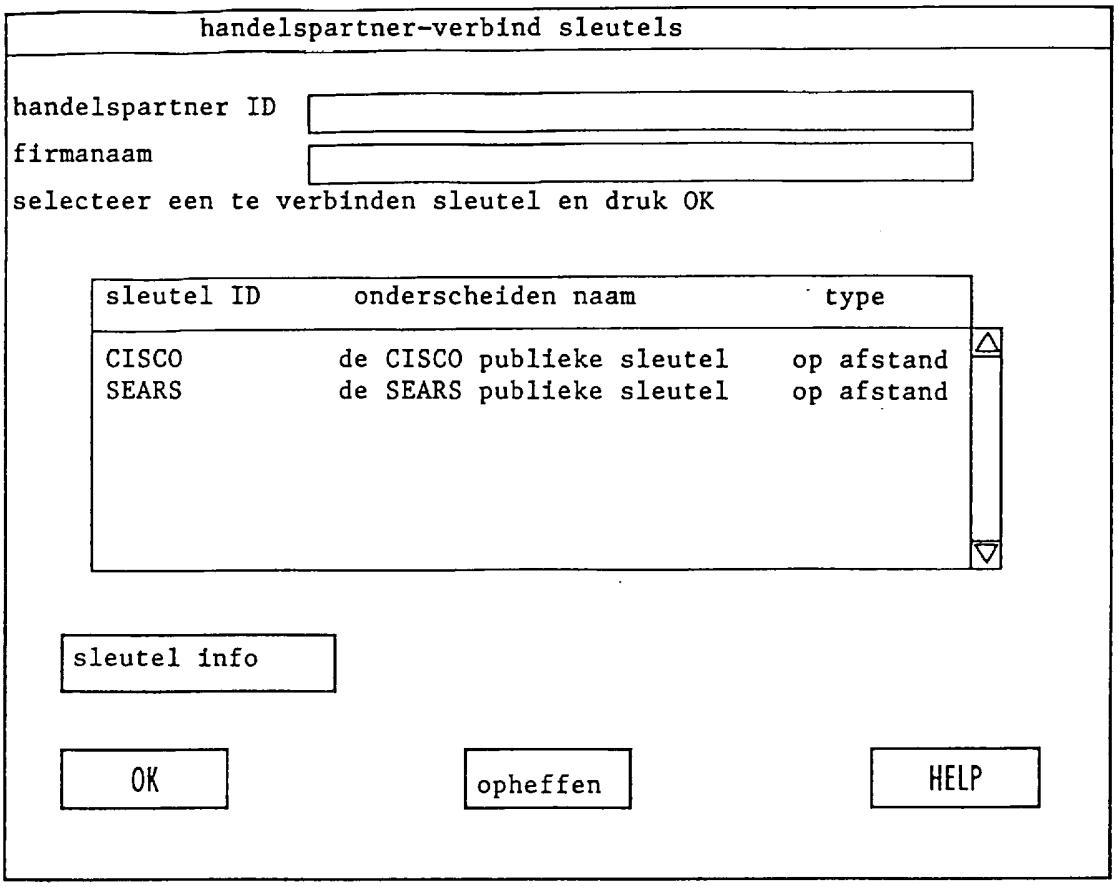
handelspartner-verbind sleutels
handelspartner ID
firmanaam
selecteer een te verbinden sleutel en druk OK
sleutel ID
onderscheiden naam
type
CISCO
de CISCO publieke sleutel
op afstand
SEARS
de SEARS publieke sleutel
op afstand
sleutel info
OK
opheffen
HELP

FIG. 20

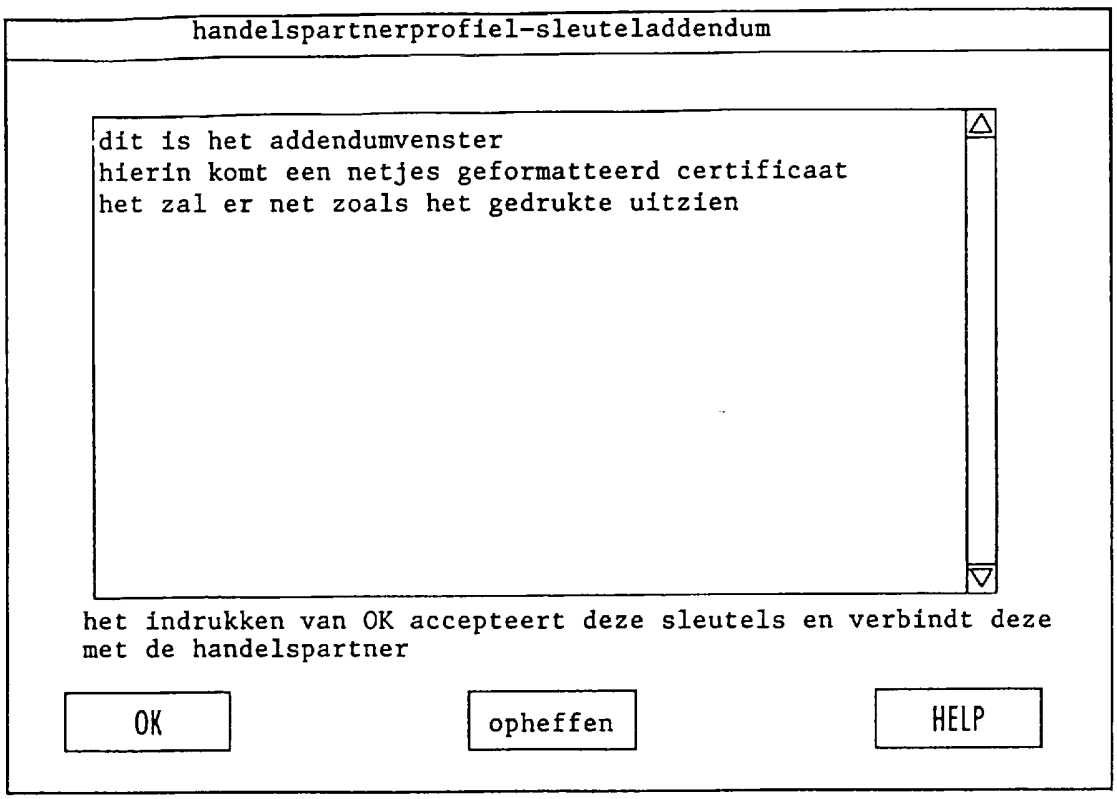
handelspartnerprofiel-sleuteladdendum
dit is het addendumvenster
hierin komt een netjes geformatteerd certificaat
het zal er net zoals het gedrukte uitzien
het indrukken van OK accepteert deze sleutels en verbindt deze met de handelspartner
OK
opheffen
HELP

FIG. 21

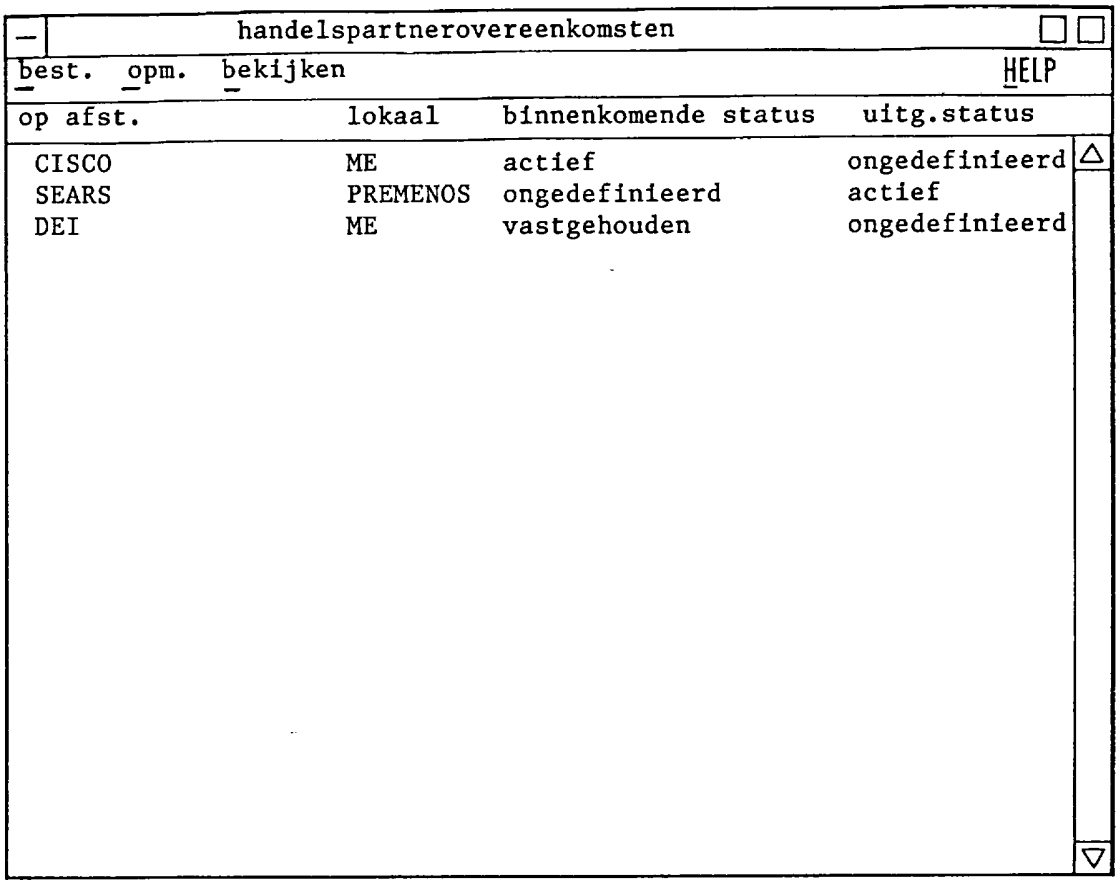
handelspartnerovereenkomsten
best. opm. bekijken
HELP
op afst.
lokaal
binnenkomende status
uitg.status
CISCO
ME
actief
ongedefinieerd
SEARS
PREMENOS
ongedefinieerd
actief
DEI
ME
vastgehouden
ongedefinieerd

FIG. 22

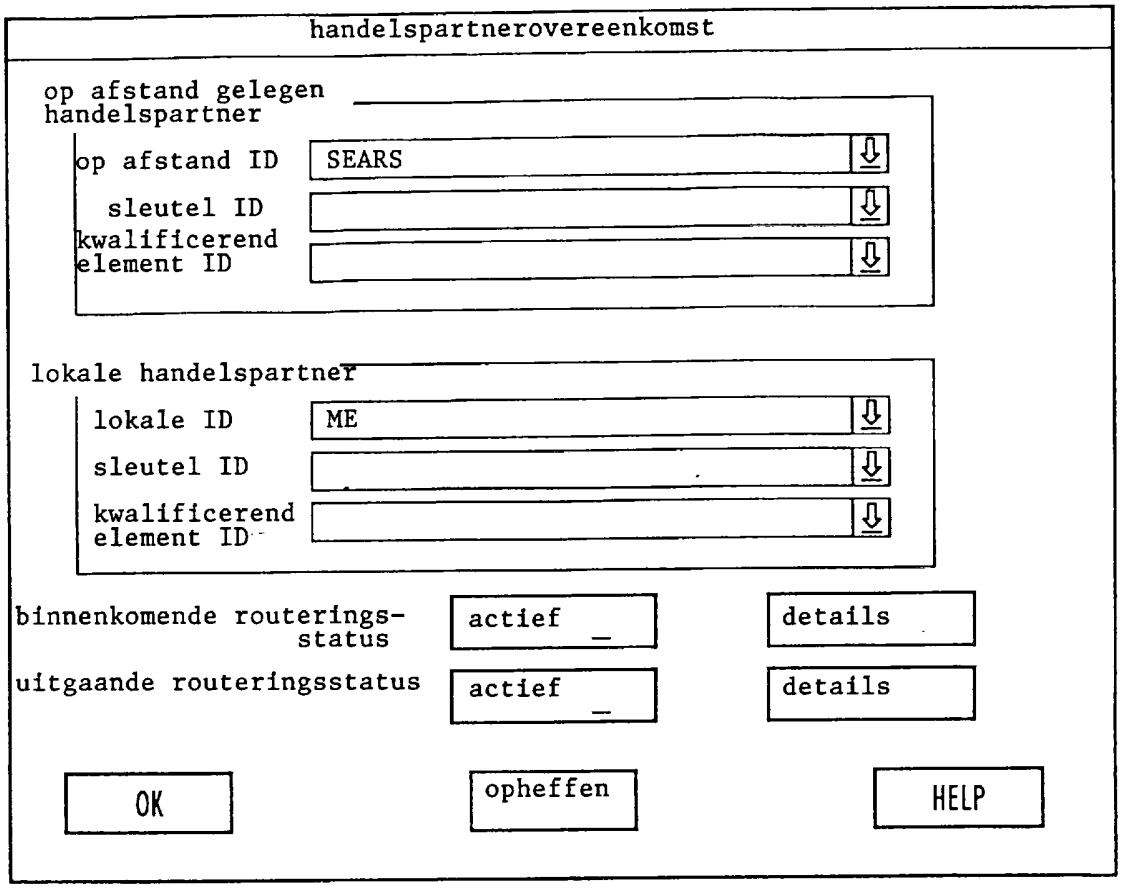
handelspartnerovereenkomst
op afstand gelegen handelspartner
op afstand ID
SEARS
sleutel ID
kwalificerend element ID
lokale handelspartner
lokale ID
ME
sleutel ID
kwalificerend element ID
binnenkomende routerings-status
actief
details
uitgaande routeringsstatus
actief
details
OK
opheffen
HELP

FIG. 23

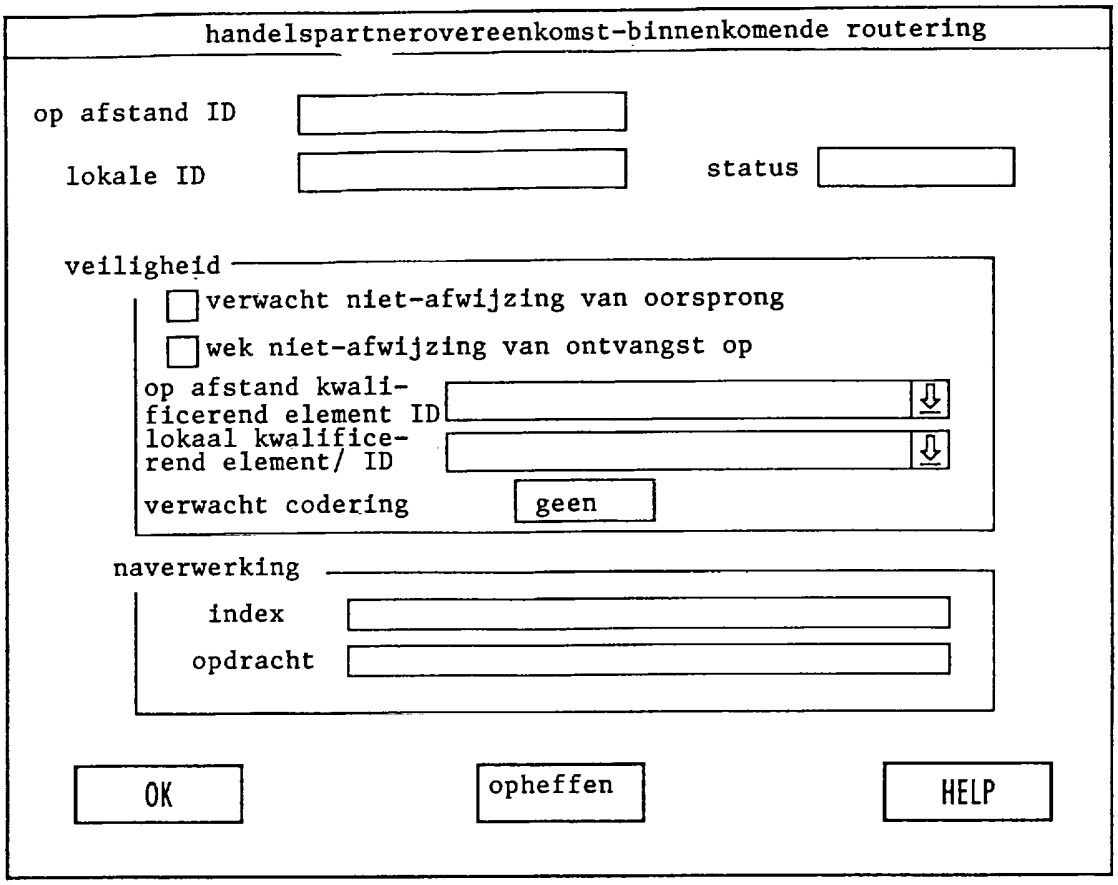
handelspartnerovereenkomst-binnenkomende routering
op afstand ID
lokale ID
status
veiligheid
verwacht niet-afwijzing van oorsprong
wek niet-afwijzing van ontvangst op
op afstand kwali-ficerend element ID
lokaal kwalifice-rend element/ ID
verwacht codering
geen
naverwerking
index
opdracht
OK
opheffen
HELP

FIG. 24

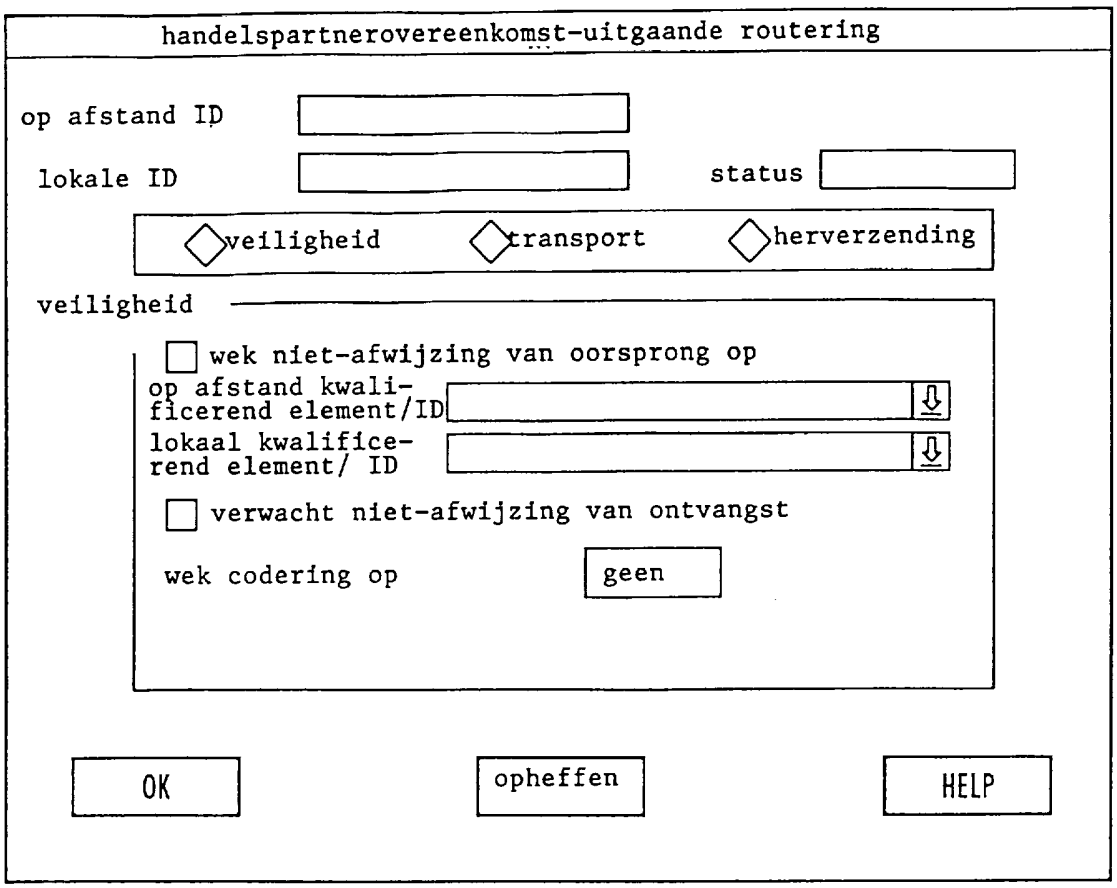
handelspartnerovereenkomst-uitgaande routering
op afstand ID
lokale ID
status
veiligheid
transport
herverzending
veiligheid
wek niet-afwijzing van oorsprong op
op afstand kwali-ficerend element/ID
lokaal kwalifice-rend element/ ID
verwacht niet-afwijzing van ontvangst
wek codering op
geen
OK
opheffen
HELP

FIG. 25

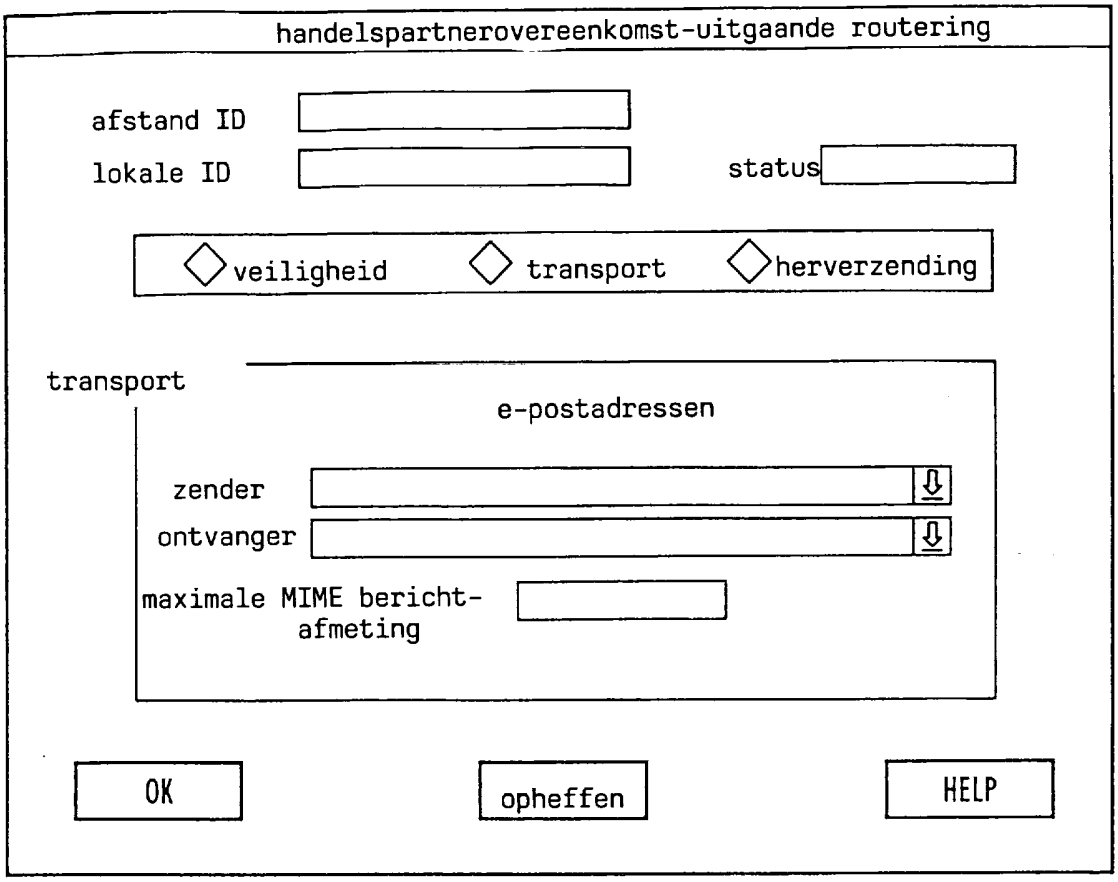
handelspartnerovereenkomst-uitgaande routering
afstand ID
lokale ID
status
veiligheid
transport
herverzending
transport
e-postadressen
zender
ontvanger
maximale MIME bericht-afmeting
OK
opheffen
HELP

FIG. 26

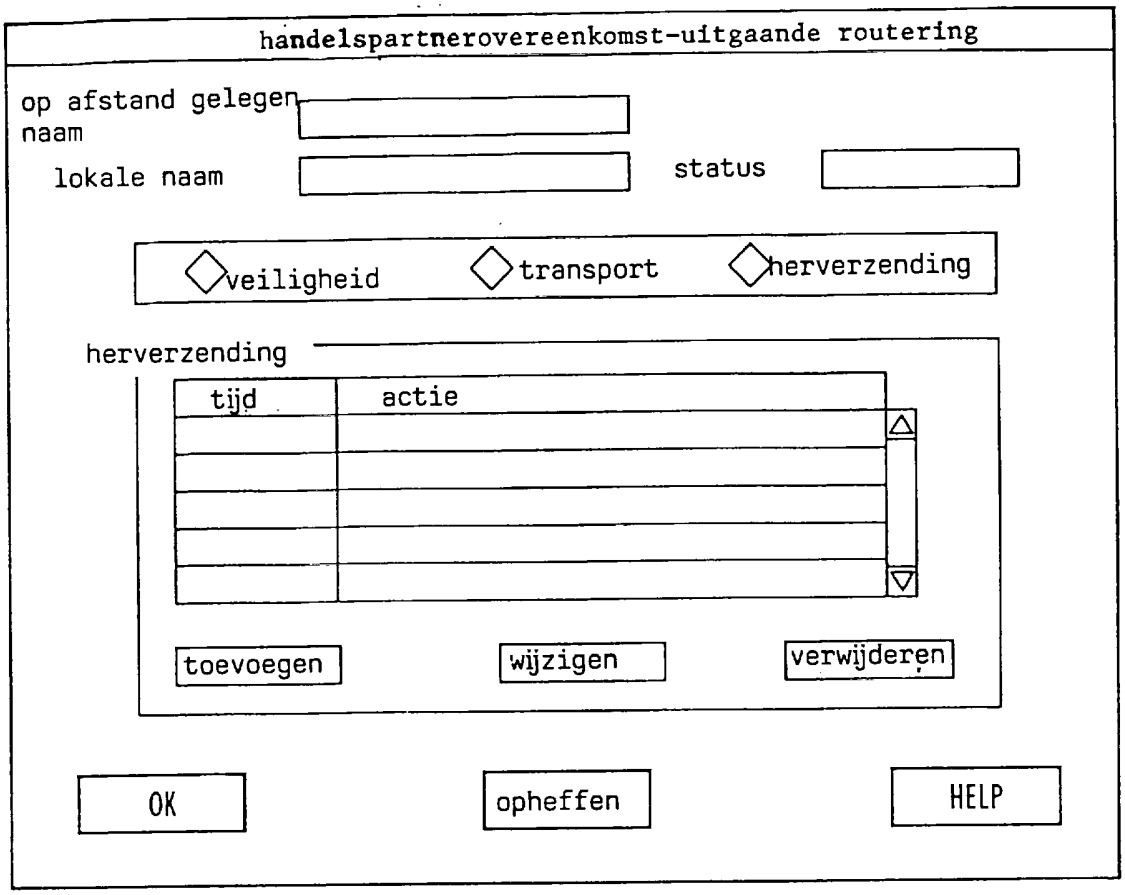
handelspartnerovereenkomst-uitgaande routering
op afstand gelegen naam
lokale naam
status
veiligheid
transport
herverzending
herverzending
tijd
actie
toevoegen
wijzigen
verwijderen
OK
opheffen
HELP

FIG. 27

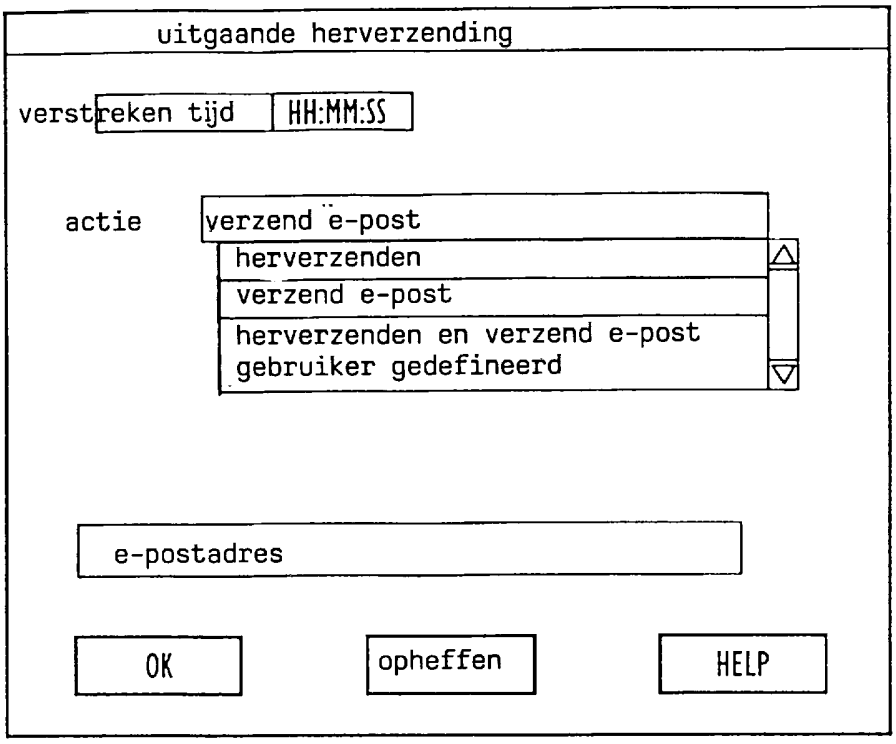
uitgaande herverzending
verstreken tijd
HH:MM:SS
actie
verzend e-post
herverzenden
verzend e-post
herverzenden en verzend e-post
gebruiker gedefineerd
e-postadres
OK
opheffen
HELP

FIG. 28

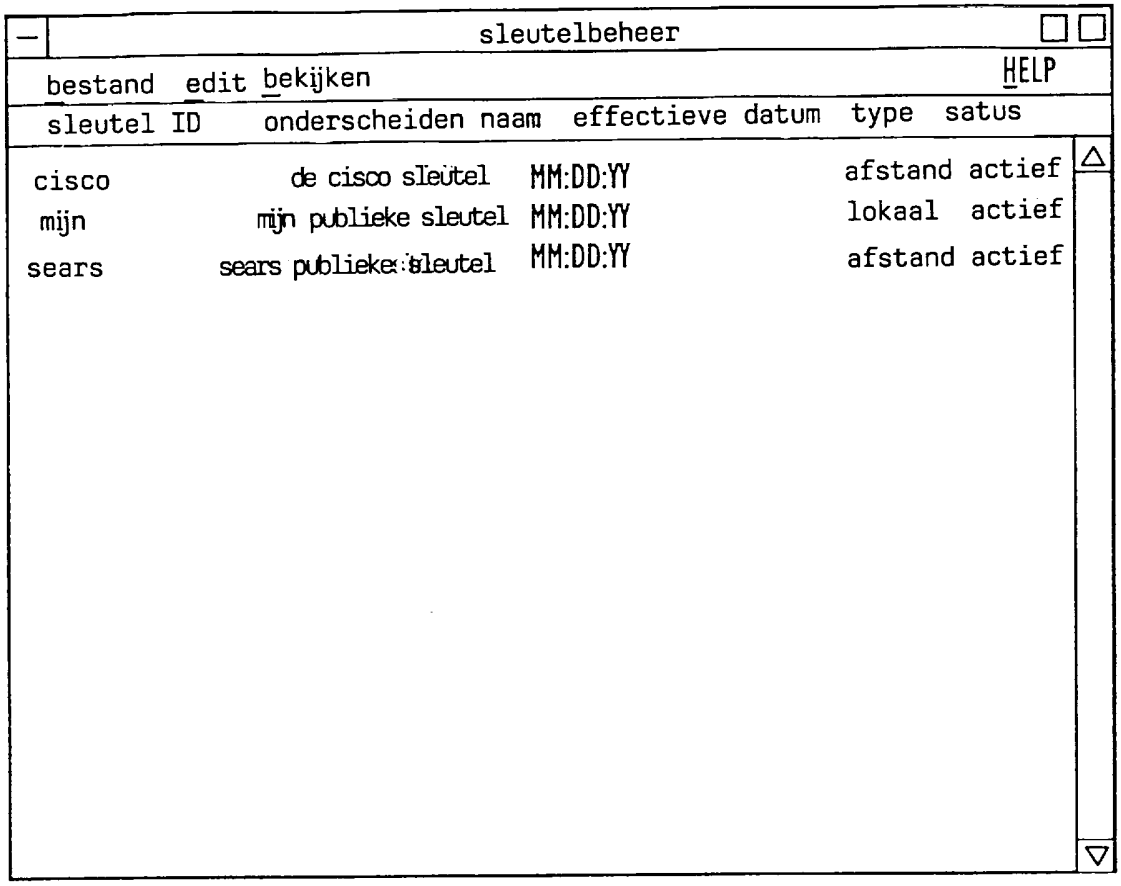
sleutelbeheer
bestand edit bekijken
HELP
sleutel ID onderscheiden naam effectieve datum type satus
cisco de cisco sleutel MM:DD:YY afstand actief
mijn mijn publieke sleutel MM:DD:YY lokaal actief
sears sears publieke sleutel MM:DD:YY afstand actief

FIG. 29

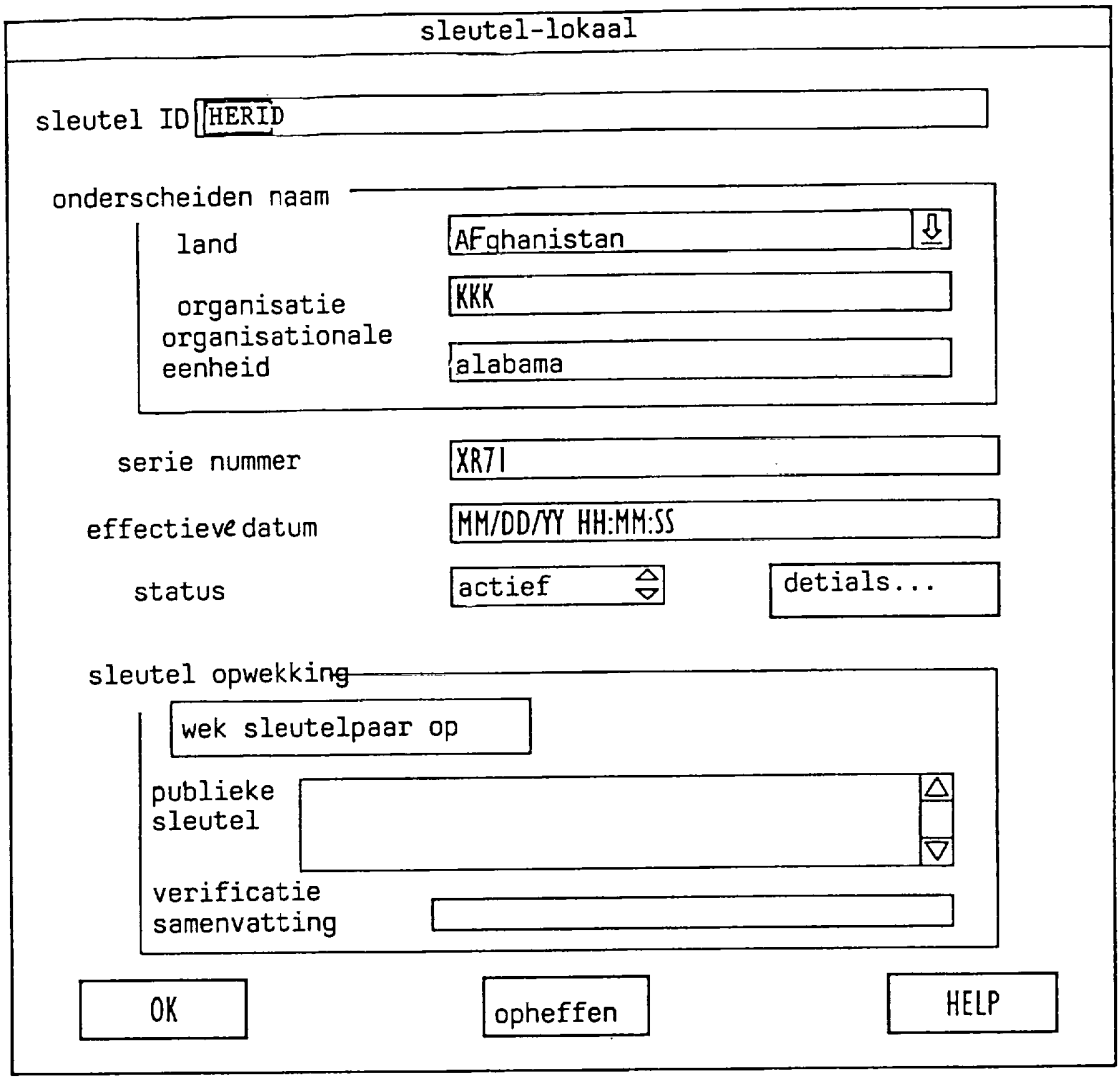
sleutel-lokaal
sleutel ID
HERID
onderscheiden naam
land
AFghanistan
organisatie
KKK
organisationale eenheid
alabama
serie nummer
XR71
effectieve datum
MM/DD/YY HH:MM:SS
status
actief
detials...
sleutel opwekking
wek sleutelpaar op
publieke sleutel
verificatie samenvatting
OK
opheffen
HELP

FIG. 30

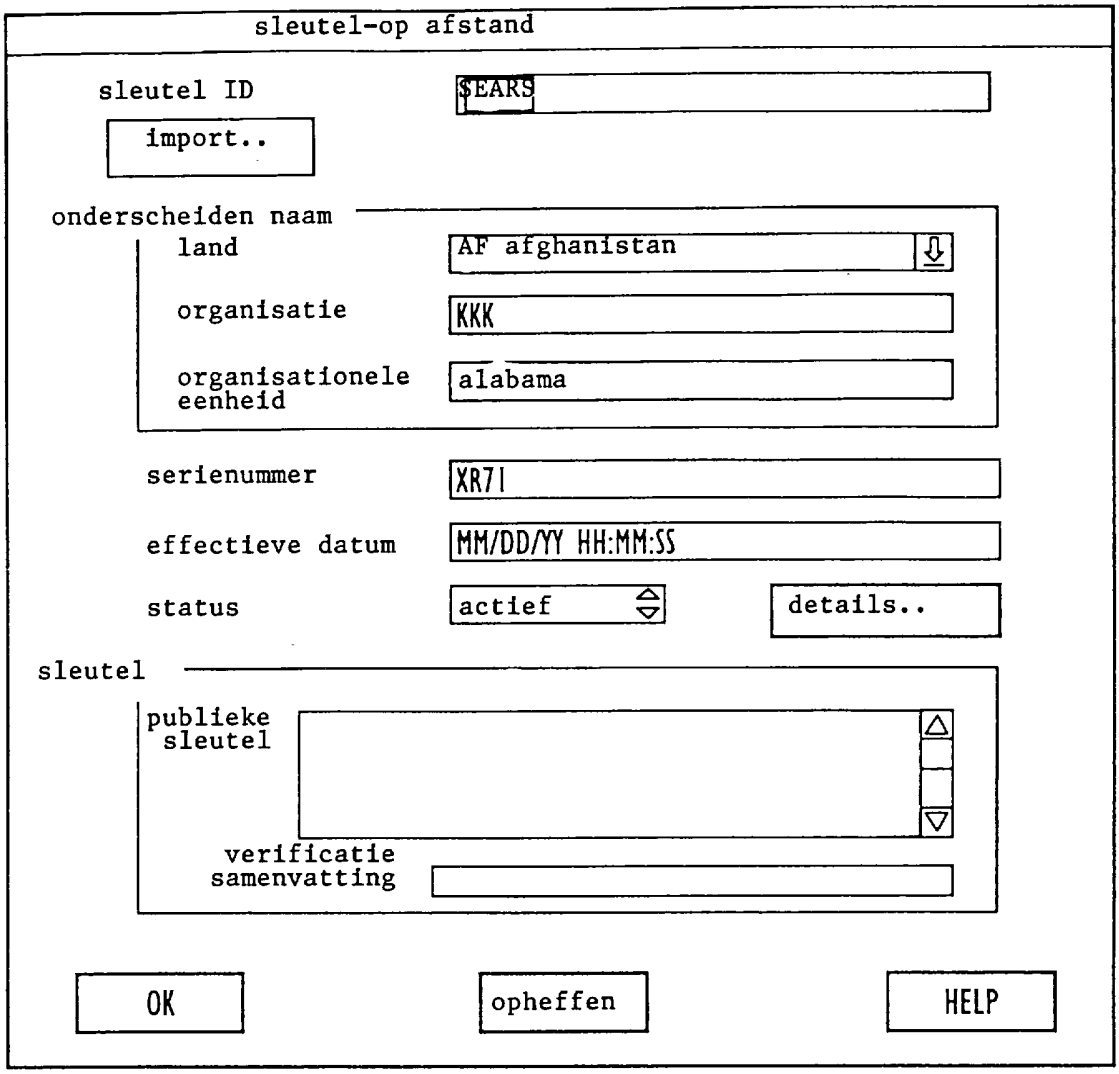
sleutel-op afstand
sleutel ID
SEARS
import..
onderscheiden naam
land
AF afghanistan
organisatie
KKK
organisationele eenheid
alabama
serienummer
XR71
effectieve datum
MM/DD/YY HH:MM:SS
status
actief
details..
sleutel
publieke sleutel
verificatie samenvatting
OK
opheffen
HELP

FIG. 31

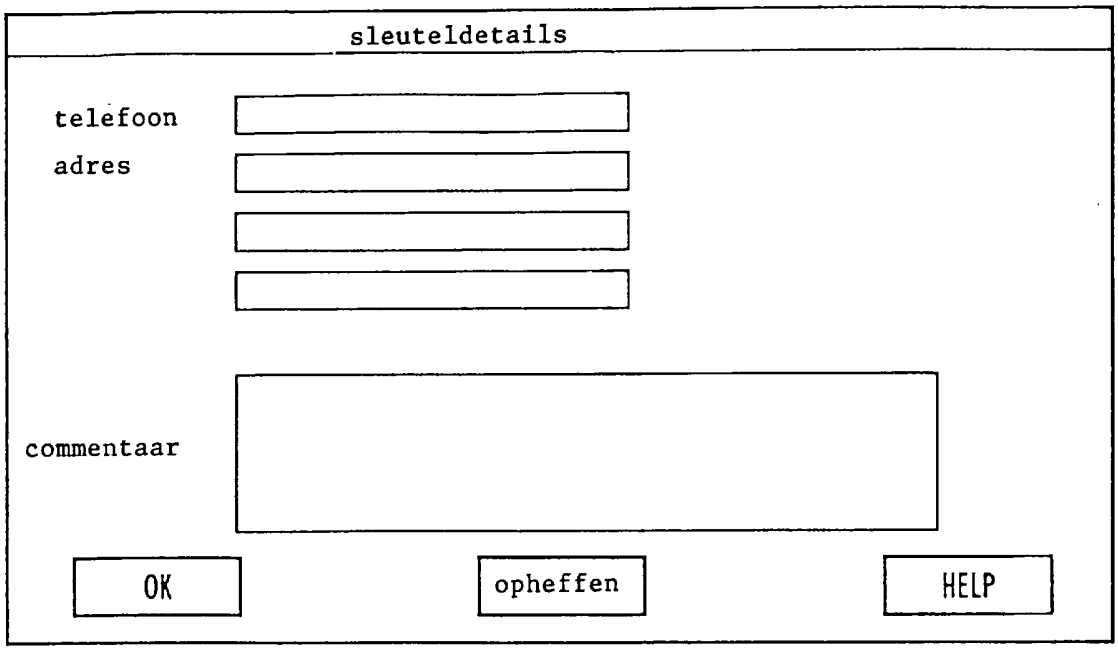
sleuteldetails
telefoon
adres
commentaar
OK
opheffen
HELP

FIG. 32

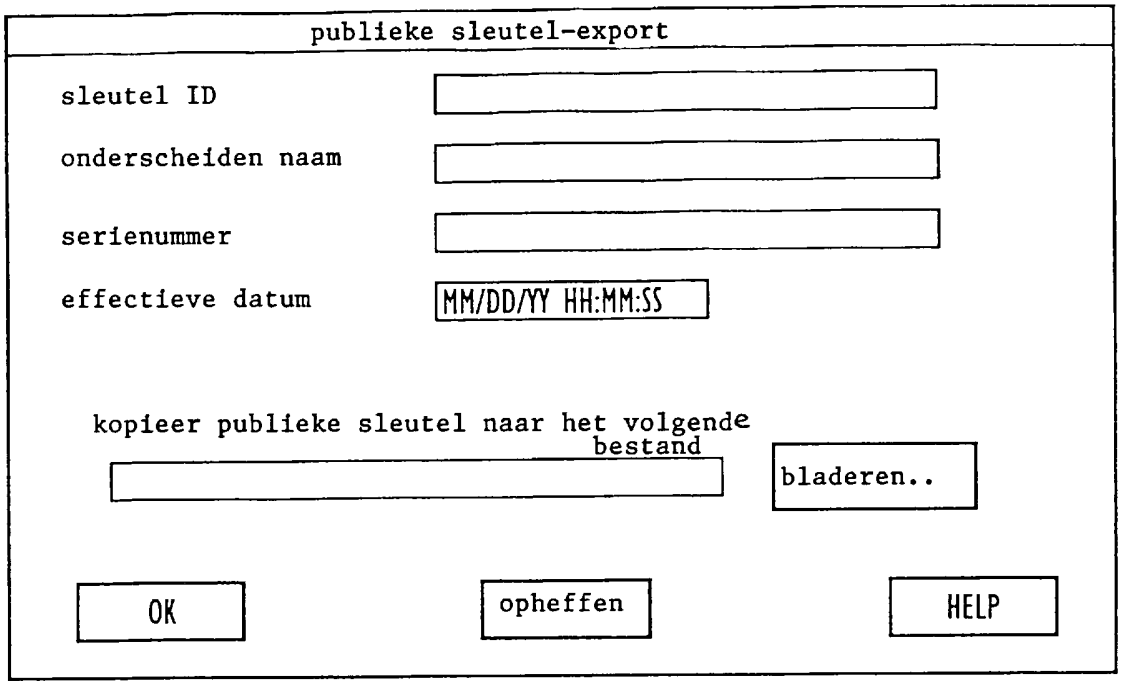
publieke sleutel-export
sleutel ID
onderscheiden naam
serienummer
effectieve datum
MM/DD/YY HH:MM:SS
kopieer publieke sleutel naar het volgende bestand
bladeren..
OK
opheffen
HELP

FIG. 33

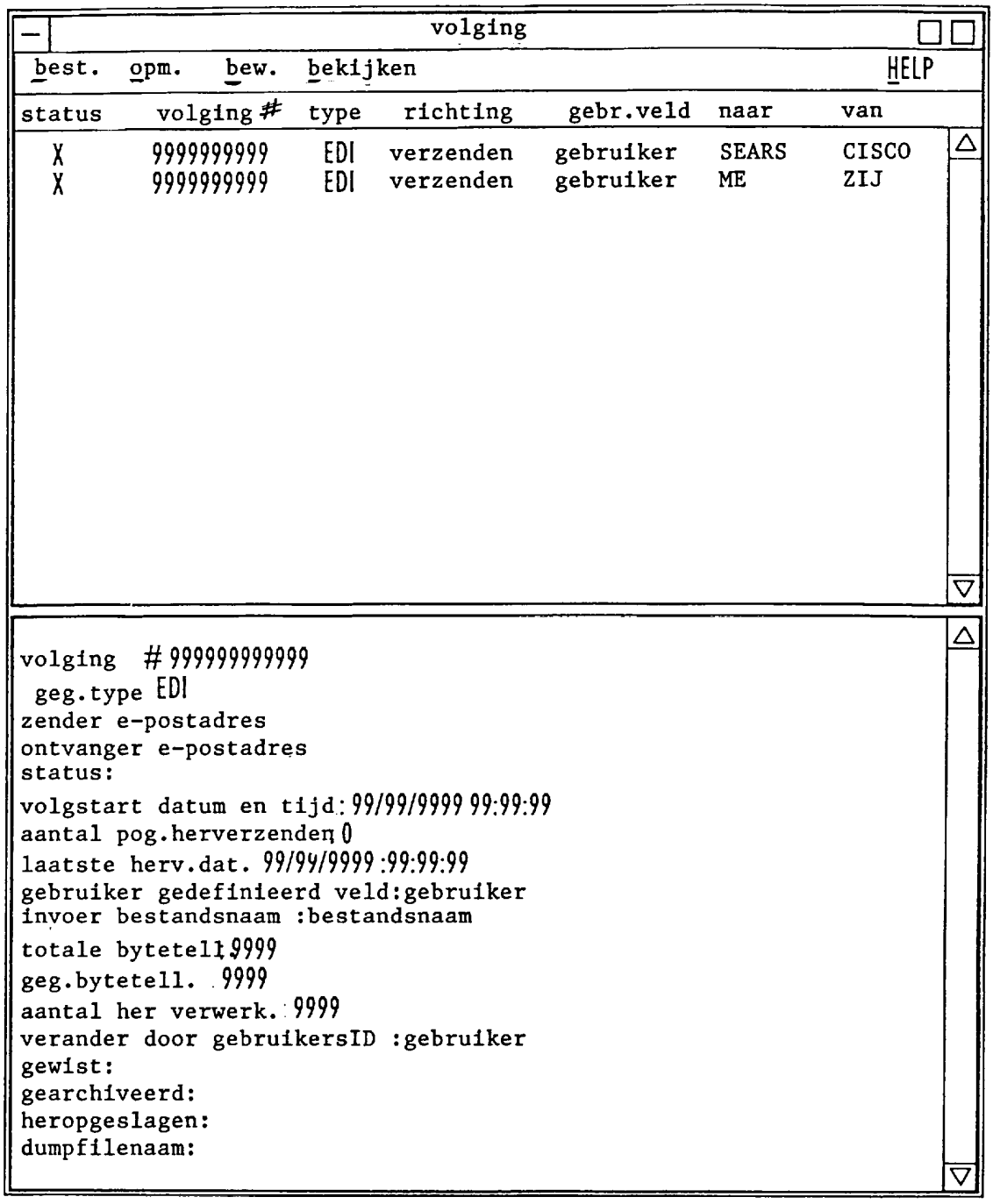
volging
best. opm. bew. bekijken HELP
status volging # type richting gebr.veld naar van
X 9999999999 EDI verzenden gebruiker SEARS CISCO
X 9999999999 EDI verzenden gebruiker ME ZIJ
volging # 999999999999
geg.type EDI
zender e-postadres
ontvanger e-postadres
status:
volgstart datum en tijd: 99/99/9999 99:99:99
aantal pog.herverzenden 0
laatste herv.dat. 99/99/9999 :99:99:99
gebruiker gedefinieerd veld:gebruiker
invoer bestandsnaam :bestandsnaam
totale bytetell. 9999
geg.bytetell. 9999
aantal her verwerk. 9999
verander door gebruikersID :gebruiker
gewist:
gearchiveerd:
heropgeslagen:
dumpfilenaam:

FIG. 34

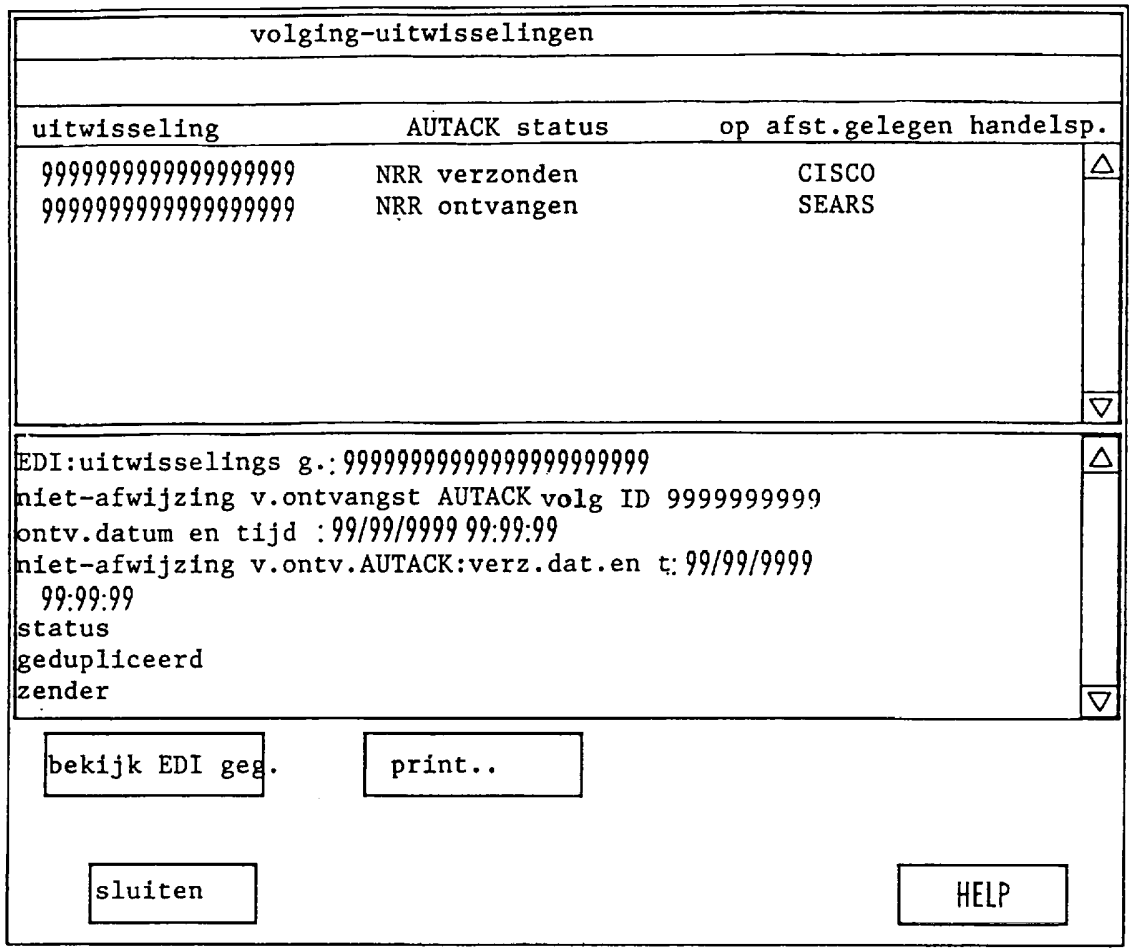
volging-uitwisselingen
uitwisseling
AUTACK status
op afst.gelegen handelsp.
9999999999999999999
NRR verzonden
CISCO
9999999999999999999
NRR ontvangen
SEARS
EDI:uitwisselings g.: 99999999999999999999999
niet-afwijzing v.ontvangst AUTACK volg ID 9999999999
ontv.datum en tijd : 99/99/9999 99:99:99
niet-afwijzing v.ontv.AUTACK:verz.dat.en t: 99/99/9999
99:99:99
status
gedupliceerd
zender
bekijk EDI geg.
print..
sluiten
HELP

FIG. 35

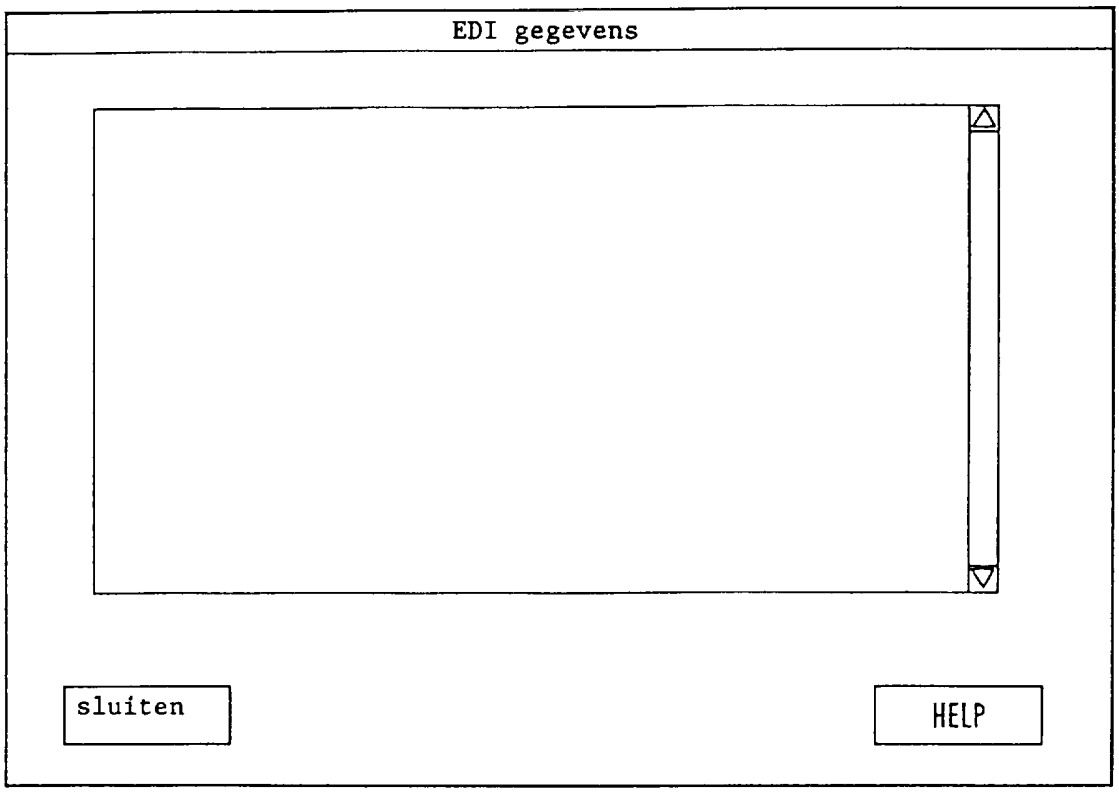

FIG. 36

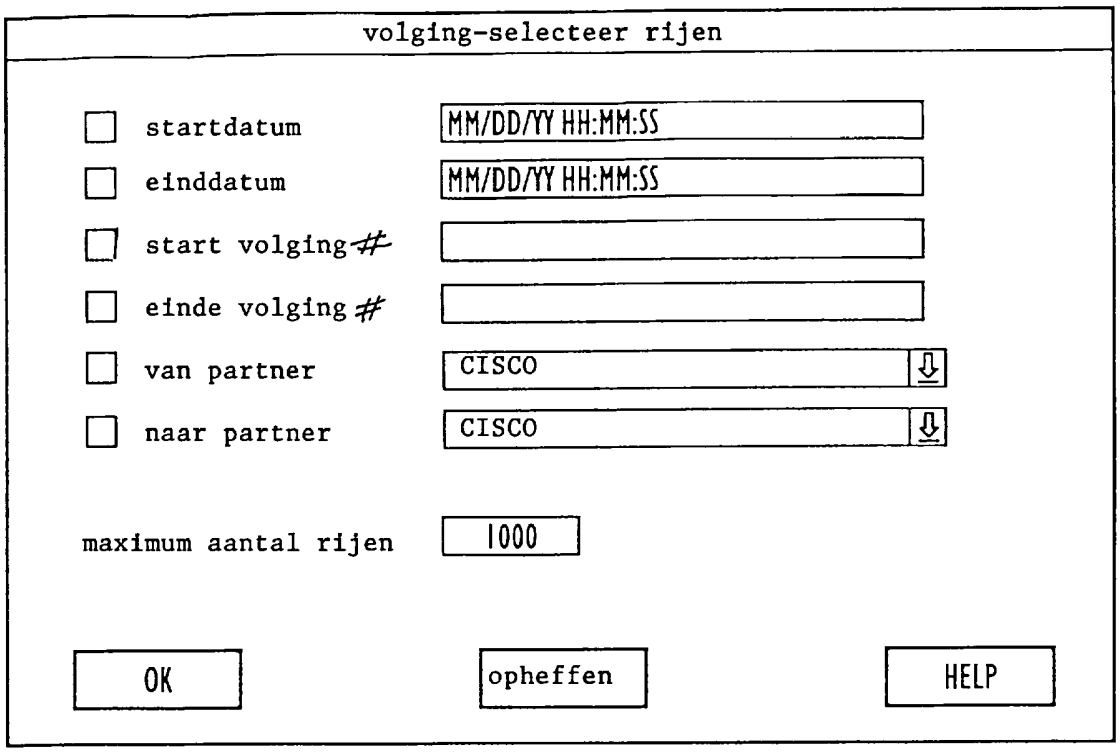
volging-selecteer rijen
startdatum
MM/DD/YY HH:MM:SS
einddatum
MM/DD/YY HH:MM:SS
start volging #
einde volging #
van partner
CISCO
naar partner
CISCO
maximum aantal rijen
1000
OK
opheffen
HELP

FIG. 37

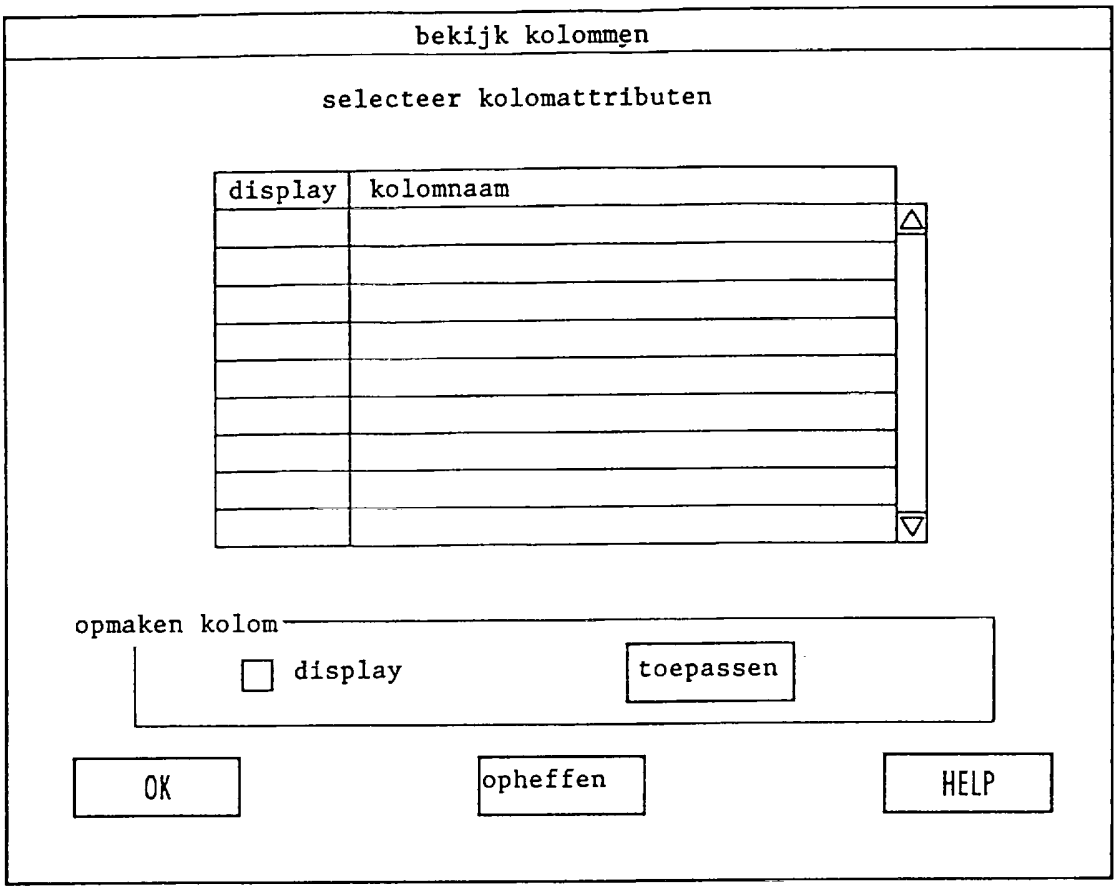
bekijk kolommen
selecteer kolomattributen
display
kolomnaam
opmaken kolom
display
toepassen
OK
opheffen
HELP

FIG. 38

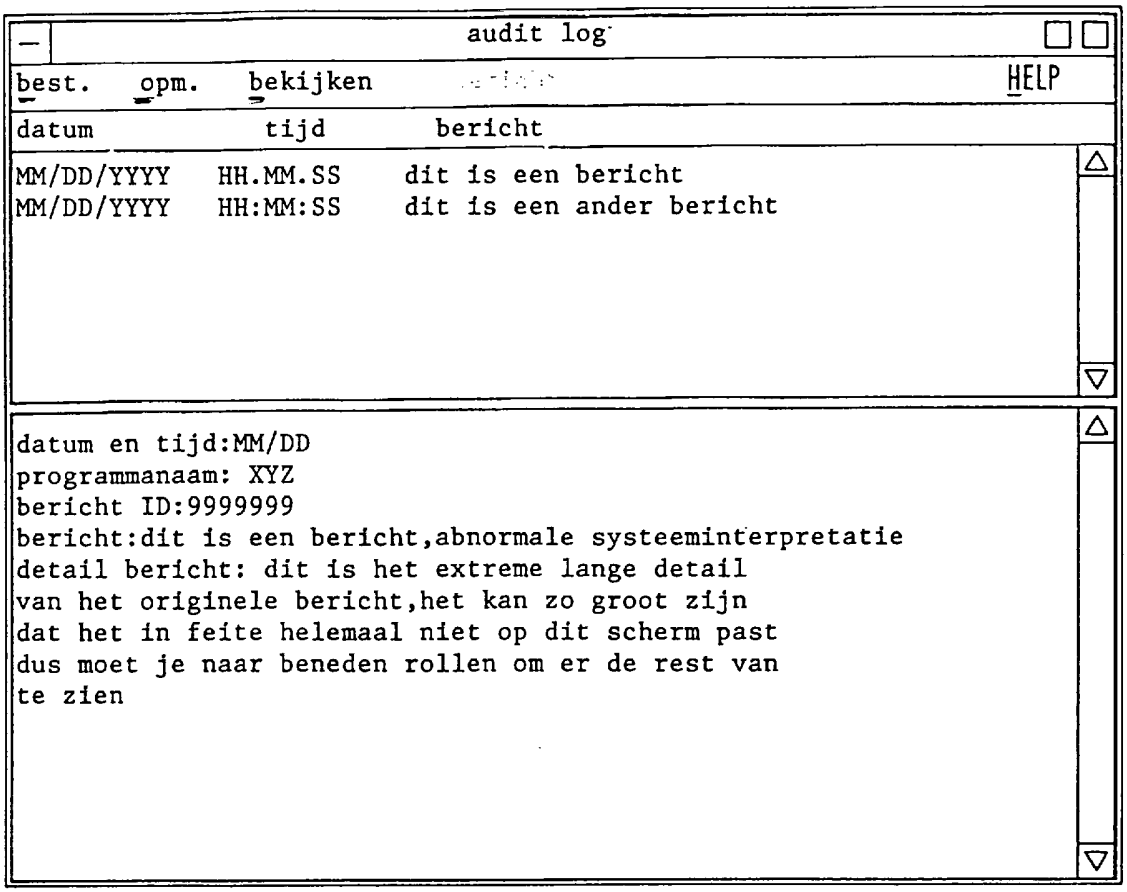
audit log
best.
opm.
bekijken
HELP
datum
tijd
bericht
MM/DD/YYYY HH.MM.SS dit is een bericht
MM/DD/YYYY HH:MM:SS dit is een ander bericht
datum en tijd:MM/DD
programmanaam: XYZ
bericht ID:9999999
bericht:dit is een bericht,abnormale systeeminterpretatie
detail bericht: dit is het extreme lange detail
van het originele bericht,het kan zo groot zijn
dat het in feite helemaal niet op dit scherm past
dus moet je naar beneden rollen om er de rest van
te zien

FIG. 39

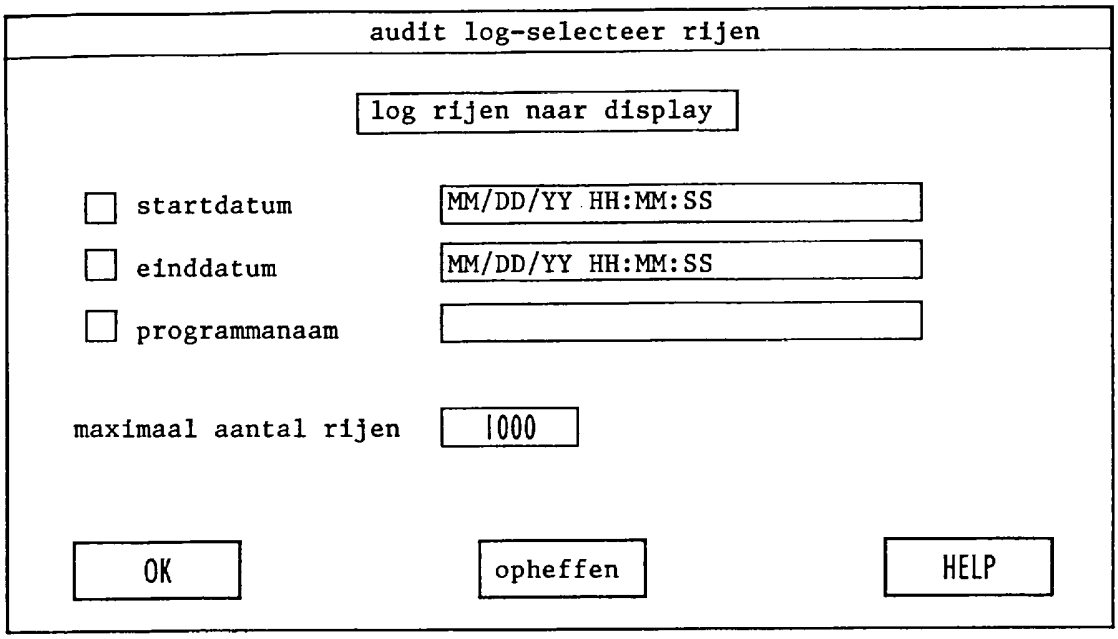
audit log-selecteer rijen
log rijen naar display
startdatum
MM/DD/YY HH:MM:SS
einddatum
MM/DD/YY HH:MM:SS
programmanaam
maximaal aantal rijen
1000
OK
opheffen
HELP

FIG. 40

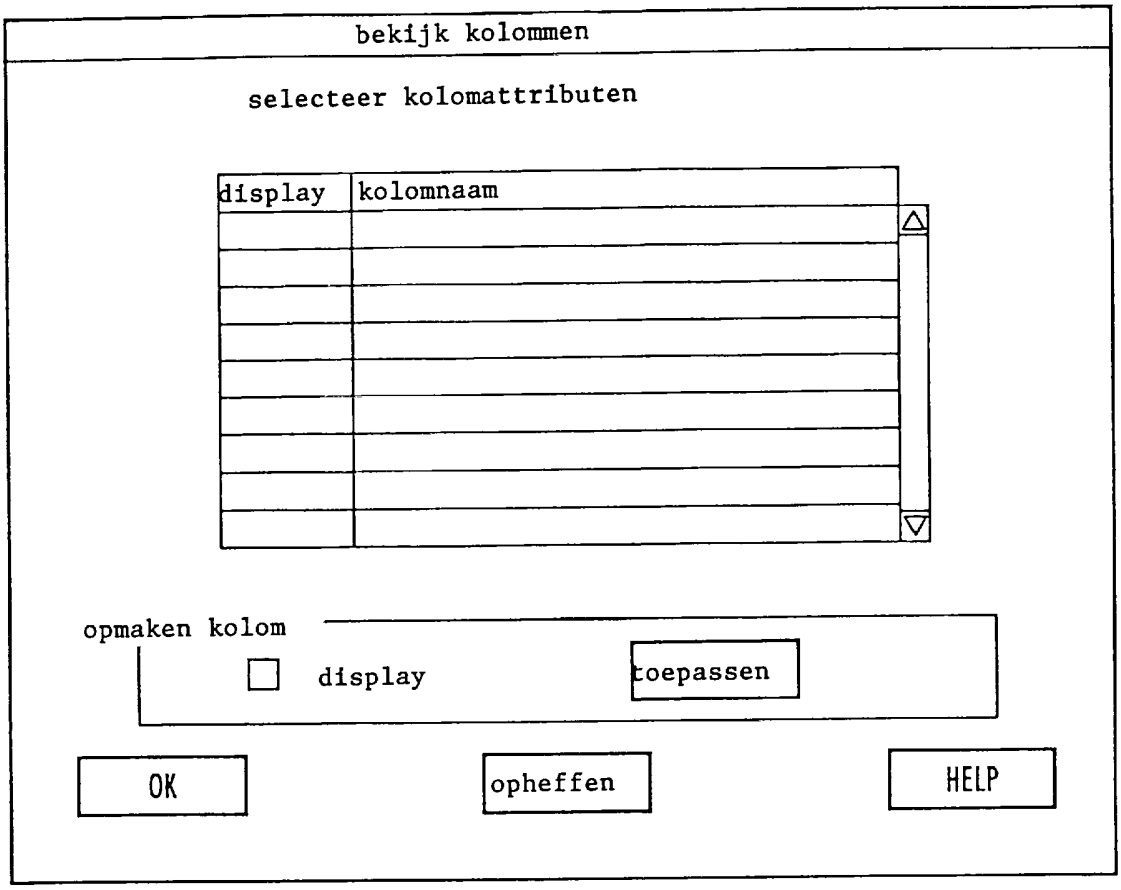
bekijk kolommen
selecteer kolomattributen
display
kolomnaam
opmaken kolom
display
toepassen
OK
opheffen
HELP

FIG. 41

Bureau voor de Industriële Eigendom

RAPPORT BETREFFENDE HET ONDERZOEK NAAR DE STAND VAN DE TECHNIEK

Octrooiaanvrage Nr.:
NO 133640
NL 1003644

VAN BELANG ZIJNDE LITERATUUR

Categorie	Vermelding van literatuur met aanduiding voor zover nodig, van speciaal van belang zijnde passages	Van belang voor conclusie(s)Nr.:	Internationale classificatie
P,Y	"EDIFACT- Secure authentication and acknowledgement message (message type AUTACK)" EDIFACT CD 9735-6 COMMITEE DRAFT, 15 Juni 1996 (1996-06-15), bladzijden 1-11, XP002112699 * alinea '05.1! * * alinea '5.3.1! * * alinea '5.3.2! * * bladzijde 9, regel 16 - regel 23 * ---	1-8,10, 13, 16-18, 26, 28-31, 34,35, 38,39, 41-45, 47-49	H04L29/06 H04L9/32
Y	US 5 005 200 A (FISCHER ADDISON M) 2 April 1991 (1991-04-02) * samenvatting * * kolom 1, regel 21 - kolom 4, regel 37 * * kolom 9, regel 35 - kolom 10, regel 49 * * kolom 15, regel 67 - kolom 16, regel 52 * * figuren 2,3,10 * --- -/--	1-8,10, 13, 16-18, 26, 28-31, 34,35, 38,39, 41-45, 47-49	**Onderzochte gebieden van de techniek** H04L G06F

Indien gewijzigde conclusies zijn ingediend, heeft dit rapport betrekking op de conclusies ingediend op :.....

2

Plaats van onderzoek	Datum waarop het onderzoek werd voltooid	Vooronderzoeker (EOB)
'S-GRAVENHAGE	19 Augustus 1999	Blanco Cardona, P

CATEGORIE VAN DE VERMELDE LITERATUUR

X : op zichzelf van bijzonder belang
Y : van bijzonder belang in samenhang met andere documenten van dezelfde categorie
A : achtergrond van de stand van de techniek
O : verwijzend naar niet op schrift gestelde van de techniek
P : literatuur gepubliceerd tussen voorrangs- en indieningsdatum
T : niet tijdig gepubliceerde literatuur over theorie of principe ten grondslag liggend aan de uitvinding
E : andere octrooipublicatie maar gepubliceerd op of na indieningsdatum
D : in de aanvrage genoemd
L : om andere redenen vermelde literatuur

& : lid van dezelfde octrooifamilie, corresponderende literatuur document

EOB FORM 02.83 (P0414)

Bureau voor de Industriële Eigendom

RAPPORT BETREFFENDE HET ONDERZOEK NAAR DE STAND VAN DE TECHNIEK

Octrooiaanvrage Nr.:
NO 133640
NL 1003644

VAN BELANG ZIJNDE LITERATUUR

Categorie	Vermelding van literatuur met aanduiding voor zover nodig, van speciaal van belang zijnde passages	Van belang voor conclusie(s)Nr.:	Internationale classificatie
A	EP 0 565 314 A (FISCHER ADDISON M) 13 Oktober 1993 (1993-10-13) * bladzijde 2, regel 30 - bladzijde 3, regel 2 * * bladzijde 8, regel 12 - regel 15 * * bladzijde 8, regel 52 - bladzijde 9, regel 14 * * bladzijde 10, regel 54 - regel 58 * * bladzijde 14, regel 48 - regel 59 * ---	1-50	
A	EP 0 516 898 A (PITNEY BOWES) 9 December 1992 (1992-12-09) * samenvatting * * kolom 1, regel 1 - regel 7 * * kolom 1, regel 52 - kolom 2, regel 10 * * kolom 3, regel 23 - regel 42 * * kolom 5, regel 21 - regel 30 * * conclusies 1,8,9 * ---	1-50	
A	SUCHUN WU: "MHS SECURITY-A CONCISE SURVEY" COMPUTER NETWORKS AND ISDN SYSTEMS, deel 25, nr. 4 / 05, 1 November 1992 (1992-11-01), bladzijden 490-495, XP000306615 ISSN: 0169-7552 * het gehele document * -----	1-50	

Onderzochte gebieden van de techniek

Indien gewijzigde conclusies zijn ingediend, heeft dit rapport betrekking op de conclusies ingediend op :.....

Plaats van onderzoek	Datum waarop het onderzoek werd voltooid	Vooronderzoeker (EOB)
'S-GRAVENHAGE	19 Augustus 1999	Blanco Cardona, P

CATEGORIE VAN DE VERMELDE LITERATUUR

X : op zichzelf van bijzonder belang
Y : van bijzonder belang in samenhang met andere documenten van dezelfde categorie
A : achtergrond van de stand van de techniek
O : verwijzend naar niet op schrift gestelde van de techniek
P : literatuur gepubliceerd tussen voorrangs- en indieningsdatum
T : niet tijdig gepubliceerde literatuur over theorie of principe ten grondslag liggend aan de uitvinding
E : andere octrooipublicatie maar gepubliceerd op of na indieningsdatum
D : in de aanvrage genoemd
L : om andere redenen vermelde literatuur
& : lid van dezelfde octrooifamilie, corresponderende literatuur document

2

EOB FORM 02 83 (P0414)

AANHANGSEL BEHORENDE BIJ HET RAPPORT BETREFFENDE HET ONDERZOEK NAAR DE STAND VAN DE TECHNIEK, UITGEVOERD IN DE OCTROOIAANVRAGE NR.

NO 133640
NL 1003644

Het aanhangsel bevat een opgave van elders gepubliceerde octrooiaanvragen of octrooien (zogenaamde leden van dezelfde octrooifamilie), die overeenkomen met octrooischriften genoemd in het rapport.
De opgave is samengesteld aan de hand van gegevens uit het computerbestand van het Europees Octrooibureau per
De juistheid en volledigheid van deze opgave wordt noch door het Europees Octrooibureau, noch door de Octrooiraad gegarandeerd ; de gegevens worden verstrekt voor informatiedoeleinden.

19-08-1999

In het rapport genoemd octrooigeschrift	Datum van publicatie	Overeenkomend(e) geschrift(en)	Datum van publicatie
US 5005200 A	02-04-1991	US 4868877 A	19-09-1989
		AT 113429 T	15-11-1994
		AT 150605 T	15-04-1997
		AU 620291 B	13-02-1992
		AU 4242589 A	13-09-1990
		CA 2000400 A,C	07-09-1990
		DE 69013541 D	01-12-1994
		DE 69013541 T	09-03-1995
		DE 69030268 D	24-04-1997
		DE 69030268 T	26-06-1997
		DK 386867 T	03-04-1995
		EP 0386867 A	12-09-1990
		EP 0586022 A	09-03-1994
		ES 2036978 T	01-01-1995
		ES 2098651 T	01-05-1997
		GR 93300050 T	30-06-1993
		JP 2291043 A	30-11-1990
		US 5214702 A	25-05-1993
		AT 122190 T	15-05-1995
		AU 2512488 A	07-09-1989
		CA 1331213 A	02-08-1994
		DE 68922422 D	08-06-1995
		DE 68922422 T	07-09-1995
		EP 0328232 A	16-08-1989
		ES 2071651 T	01-07-1995
EP 0565314 A	13-10-1993	AU 3560793 A	07-10-1993
		CA 2093094 A	07-10-1993
		JP 6295286 A	21-10-1994
		US 5390247 A	14-02-1995
		US 5337360 A	09-08-1994
EP 0516898 A	09-12-1992	CA 2043533 A,C	01-12-1992
		JP 6014018 A	21-01-1994
		US 5022080 A	04-06-1992

Algemene informatie over dit aanhangsel is gepubliceerd in de 'Official Journal' van het Europees Octrooibureau nr 12/82 blz 448 ev