Technische aspecten, standaarden en richtlijnen

m.b.t.

EDI & Internet

in de agrarische sector

i.s.m. EDI Agro Vereniging

Januari 2002

Colofon

Uitgever
Praktijkonderzoek Veehouderij
Postbus 2176, 8203 AD Lelystad
Telefoon 0320 - 293 211
Fax 0320 - 241 584
E-mail info@pv.agro.nl.
Internet http://www.pv.wageningen-ur.nl

Redactie en fotografie
Praktijkonderzoek Veehouderij

Aansprakelijkheid
Het Praktijkonderzoek Veehouderij aanvaardt geen aansprakelijkheid voor eventuele schade voortvloeiend uit het gebruik van de resultaten van dit onderzoek of de toepassing van de adviezen

Bestellen
ISSN 0169-3689
Eerste druk 2002/oplage 50
Prijs € 17,50 (f 38,56)

Losse nummers zijn schriftelijk, telefonisch, per E-mail of via de website te bestellen bij de uitgever.

PRAKTIJKONDERZOEK VEEHOUDERIJ

EDI AGRO VERENIGING
VERENIGING VOOR ICT IN DE AGRARISCHE SECTOR

Technische aspecten, standaarden en richtlijnen

m.b.t.

EDI & Internet in de agrarische sector

EAV werkgroep EDI & Internet:

Aaken, C. van (Van Aaken Automatisering)
Graumans, C. (Agrotel)
Holster, H. (Praktijkonderzoek Veehouderij, afd. Agrarische Telematica)
Land, B. van't (CR-Delta)
Loosveld, S. (Comvee Boerderij-Automatisering)
Meinema, R. (Rovecom)
Romme, R. (IPG/TOPIGS)

Januari 2002

Voorwoord

In de Nederlandse veehouderij wordt al sinds eind jaren 90 (vorige eeuw) gesproken over het Internet als transportmedium voor EDI berichtenverkeer. Ook uit deze tijd stammen de eerste initiatieven waarbij gegevensuitwisseling over internet is gaan lopen, in de melkveehouderij zijn inmiddels de ftp-servers van Zuivelnet en NRS algemeen bekend.
Een groot deel van de veehouders heeft inmiddels toegang tot Internet, binnen afzienbare tijd zal dit medium, ook voor de bedrijfsvoering op het agrarische bedrijf, een algemeen goed zijn geworden.
Nieuw te ontwikkelen EDI-toepassingen zullen waarschijnlijk alleen nog gebruik maken van het Internet. Van de bestaande berichten kan worden gezegd dat ze de komende tijd zullen migreren naar een internetomgeving, waarbij ook de oude infrastructuur daar nog wel even naast zal blijven bestaan.

Vanuit de traditie van standaardisatie in de veehouderij is er sterke behoefte ontstaan tot onderzoek en afspraken m.b.t. het gebruik van EDI over Internet. Tot dusver ontwikkelde elk toepassingsgebied (althans een aantal) zijn eigen oplossing. Daarnaast is er het inzicht ontstaan dat veiligheden en zekerheden op Internet niet als vanzelfsprekend zijn geregeld en dat in een tijd waarbij het belang van beveiliging en bevestiging (borging) nu juist een enorme vlucht neemt.
De EDI Agro Vereniging (EAV) heeft, als belangenvereniging van de EDI gebruikersgroepen, in 2000 een interne werkgroep geformeerd en deze de opdracht meegegeven om te werken aan afspraken over technische aspecten rondom EDI & Internet. De werkgroep is samengesteld uit een doorsnee van het softwarebedrijfsleven en gegevensuitwisselende organisaties in zowel de rundveehouderij- als ook de varkenshouderijsector.
Het Praktijkonderzoek Veehouderij (ATC) is gevraagd het project te leiden. Bijdrage van het PV is tot stand kunnen komen in het kader van het project “hergebruik en beveiliging van kritische informatie”, een project dat zowel in de melkveehouderij als ook in de varkenshouderij door de productschappen wordt gefinancierd.

De werkgroep heeft nu met het uitkomen van dit rapport haar taak volbracht. Gaandeweg het onderzoek is gebleken dat de opdracht tamelijk complex was. Sterke behoefte was er om voortdurend in- en tegelijk ook uit te zoomen in de tijd. De korte termijn problematiek en behoeften zijn uiteraard heel anders dan die op de lange termijn, toch bleek steeds weer dat een en ander vaak moeilijk te scheiden is. Het is uiteindelijk onvermijdelijk gebleken om de problematiek gefaseerd in de tijd te leggen, daarbij is ook niet voorbijgegaan aan de ontwikkelingen op de langere termijn, alhoewel dit niet direct onderdeel van de opdracht was.

Dat het heeft kunnen komen tot een onzes inziens gestructureerd en voor de praktijk bruikbaar rapport is te danken aan de ijverige inzet van velen uit de sector. Niet alleen de werkgroepleden zelf, maar ook hun achterban en daarnaast nog vele andere partijen hebben meegewerkt aan de totstandkoming van dit product. Het zijn er te veel om op te noemen, maar veel dank is hen zeker verschuldigd.

Tot slot moet de wens worden uitgesproken dat het rapport, en in het bijzonder de praktische afspraken en handvatten daar in, draagvlak zal vinden in de veehouderij, wellicht in de gehele agrarische sector of zelfs daarbuiten. Electronische communicatie is immers een zaak van samenwerking, en dat steeds vaker over de grenzen van branches en landen heen.

Henri Holster

Projectleider en secretaris
EAV werkgroep EDI & Internet

Samenvatting

Electronische gegevensuitwisseling liep tot voor kort uitsluitend via Value Added Networks (VAN). De beschermde omgeving van de X400 netwerken maakt plaats voor het wereldwijde Internet als medium waarover de EDI berichten lopen. Internet brengt echter nieuwe bedreigingen met zich mee en vraagt tegelijk om nieuwe afspraken over het gebruik ervan. In opdracht van de EDI-Agro Vereniging (EAV) heeft een werkgroep zich gebogen over een aantal technische aspecten van EDI & Internet met als belangrijkste doel te komen tot een set van richtlijnen over het gebruik ervan. Een viertal samenhangende aspecten zijn onderzocht: ontwikkeling van een generieke envelop, beveiligingsaspecten, retourberichten en een beschouwing m.b.t. de huidige EDI-toepassingen over Internet.

Electronische gegevensuitwisseling (over Internet) zal een ontwikkeling doormaken. De werkgroep voorziet een groeipad voor de komende jaren, welke zich laat beschrijven in een aantal fasen. Nu al vindt er gegevensuitwisseling over Internet plaats, veelal nog tamelijk ongecontroleerd of in ieder geval niet gestuurd door gemeenschappelijke richtlijnen (fase 0). In fase 1 zullen er gemeenschappelijke technische afspraken gelden over hoe om te gaan met zaken als transport, beveiliging e.d. Het EDI-bericht blijft nog ongewijzigd van opzet en gebruikte syntax, alleen het transport loopt nu over Internet. De volgende fase is die van het gebruik van een generieke architectuur voor de afhandeling van het berichtenverkeer. De basis hiervan wordt gevormd door een generieke envelop, zeer goed mogelijk is dit de ebXML envelop. Fase 4 wordt tot slot gezien als een volwaardige e-business-omgeving waarbij bedrijfsprocessen dynamisch met elkaar communiceren, gebruikmakend van het volledige ebXML concept.

Vanuit de uitgangspunten dat een nieuwe generieke envelop duurzaam maar ook transport- en berichtonafhankelijk moet zijn is het onderzoek terecht gekomen op het pad van de kersverse ebXML standaard. In een subcommissie is nader onderzoek uitgevoerd naar de toepasbaarheid van deze standaard in de agrarische EDI-toepassingen, met name gericht op de toepassing van de ebXML envelop. De ebXML standaard blijkt zeer zeker geschikt. Kanttekening hierbij is dat de praktische implementatie ervan wel afhankelijk is van (nog niet of amper) beschikbare tools. EAV zou eventueel wel per direct kunnen kiezen voor de ebXML envelop maar zal dan zelf een tool moeten ontwikkelen voor de juiste verwerking van de berichten c.q. envelop.
Omdat het nu als niet opportuun wordt beschouwd om de huidige berichtheaders te herijken is daar voor de korte termijn geen verdere aandacht aan besteed.

Beveiliging van berichtenverkeer berust, net zoals in de niet-electronische zakelijke wereld, op vertrouwen en betrouwbaarheid. Een aantal methoden voor verhoging van de betrouwbaarheid worden behandeld. Van groot belang in dit kader is de risicobeheersing. De beschreven instrumenten risicoanalyse en classificatie kunnen als handvatten dienen om de risico's te kwantificeren en de daarbij horende maatregelen te onderkennen. Het gebruik van deze hulpmiddelen wordt aanbevolen, te meer omdat daarmee het beveiligingsbewustzijn wordt versterkt.

Retour- of bevestigingsberichten zijn er in een aantal varianten. Met de onzekerheden van het Internet, maar onder andere ook de toenemende behoefte aan borging, worden deze berichten steeds belangrijker. Berichten voor ontvangst- en verwerkingsbevestigingen op berichtniveau zijn beschreven voor de EDI-syntaxen EDIFACT en ADIS. Bevestigingsberichten op regel/record-niveau zijn bijna niet generiek te beschrijven, daarnaast worden deze in veel gevallen als te gedetailleerd en daarmee soms als minder gewenst beschouwd. Daar waar er behoefte is aan bevestiging op recordniveau zal dit binnen de EDI-standaard zelf gedefinieerd kunnen worden.

Een inventarisatie is uitgevoerd van de huidige EDI-toepassingen over Internet. In de melkveehouderijsector zijn een aantal FTP-toepassingen actief die zorgen voor het transport van EDI berichten over het Internet. In de varkenshouderijsector zien we juist het gebruik van e-mail als transportmedium voor EDI berichten, veelal gericht op de bediening van de buitenlandse klant. Vergelijken we de eigenschappen van FTP met die van SMTP (e-mail) dan zien we wel theoretische verschillen, in de praktijk blijkt het verschil vaak minder groot. De keus voor FTP dan wel voor SMTP zal dan ook niet altijd gebaseerd zijn op de feitelijke eigenschappen ervan.
Door EAN Nederland is het gebruik van EDI berichten via e-mail attachments onderzocht. E-mail blijkt hiervoor goed bruikbaar te zijn. Een aantal gebruiksregels zijn opgesteld voor het afhandelen van EDI-berichten als attachment. Aan EAV wordt voorgesteld deze regels, met een enkele specifieke aanvullende richtlijn, over te nemen.
Aanbevelingen die de werkgroep aan EAV doet zijn onder andere het implementeren van de eerder genoemde gebruiksregels en het ontwerpen van een generieke envelop op basis van ebXML zodra hiervoor de benodigde tools beschikbaar komen. Voor de lange termijn wordt geadviseerd om het vizier te richten op de ebXML standaard, waarbij er speciale aandacht uitgaat naar zaken als nader onderzoek naar inrichting van ebXML componenten, de ontwikkeling van een proof of concept en de inrichting van een beheersstructuur inclusief de opzet van een agrarische repository.

Summary

Until recently, electronic data exchange was solely via Value Added Networks (VAN). The protected environment of the X400 networks has been superseded by the worldwide Internet as the medium for sending EDI messages. Internet has brought new risks, however, and requires new agreements about its use, which is why a working group was commissioned by *EDI-Agro Vereniging* (EAV) to examine various technical aspects of EDI and Internet, with the main aim of producing a set of guidelines for their use. The four aspects examined were: the development of a generic envelope, security, replies, and a survey of current EDI applications relating to Internet.

Electronic data exchange (over the Internet) will develop further. The working group foresees that growth in the coming years will be in a number of phases. Data exchange is already occurring over the Internet, largely unregulated, or not in accordance with communal guidelines (phase 0). In phase 1, communal technical agreements will be made about how to deal with matters such as transmission, security, etc. The EDI message will remain unchanged in purpose and syntax, but transmission will be via the Internet. The next phase involves using a generic architecture for the sending and receiving of messages. This will be based on a generic envelope, very probably the ebXML envelope. Finally, phase 4 is envisaged as a fully-fledged e-business environment, enabling company processes to communicate with each other dynamically, making use of the full ebXML concept.

Assuming that a new generic envelope will be durable and independent of transmission and message, research was done on the new ebXML standard. A subcommittee further investigated the applicability of this standard in agrarian EDI applications, particularly relating to the application of the ebXML envelope. The ebXML standard was found to be very suitable. It should be noted, however, that its implementation in practice depends on tools that are as yet unavailable, or are difficult to obtain. EAV could immediately opt for the ebXML envelope, but would then have to develop a tool for the correct processing of the messages and envelope. As it was felt that the time was not ripe for recalibrating the present message headers, it was decided not to pay further attention to this in the short term.

As is the case in the non-electronic world of business, the security of sending and receiving messages rests on trust and reliability. Several methods for improving security are discussed. Risk management is very important in this context. The tools for managing and classifying risk can serve as a basis for quantifying risks and identifying which measures are required. The use of these aids is recommended, especially as they enhance awareness of security.

There are various reply or confirmation of receipt messages. They are becoming more important because of the uncertainties of Internet and also because of the growing need for assurance. At message level, messages to confirm receipt and messages to confirm that action is being taken have been written for the EDI syntaxes EDIFACT and ADIS. It is almost impossible to generically describe confirmatory messages at line or record level; furthermore, in many cases these messages are deemed to be too detailed and thus less desirable. Where a confirmatory message is required at record level, this can be defined within the EDI standard itself.

An inventory of current EDI applications relating to Internet reveals that some FTP applications are active in the Dutch dairy-farming sector to transmit EDI messages over the Internet. In the Dutch pig-keeping sector, e-mail is being used as the medium to transmit EDI messages, with much being directed to serve clients outside the Netherlands. A comparison of the properties of FTP with those of SMTP (e-mail) reveals theoretical differences, but in practice the difference is often much less. Whether FTP or SMTP is chosen will therefore not always depend on the actual properties of these systems.

EAN Nederland has studied the use of EDI messages via e-mail attachments and has found that e-mail is very usable for this. Some rules for users have been drawn up for dealing with EDI messages sent as attachments. It is proposed that EAV adopt these rules, with a single specific complementary guideline.

The working group's recommendations to EAV include the implementation of the users' rules mentioned above, and the development of a generic envelope on the basis of ebXML as soon as the tools needed for this become available. For the long term it is advised to focus on the ebXML standard, paying special attention to matters such as further research on the design of ebXML components, the development of a proof of concept, and the design of a management structure, including the setting up of an agrarian data repository.

Inhoudsopgave

1 Inleiding

EDI, ofwel electronische gegevensuitwisseling, gebeurde tot voor kort amper via het Internet, maar via VAN's (Value Added Networks). Een VAN is een besloten netwerk welk doorgaans gekwalificeerd kan worden als veilig en betrouwbaar.
Met de komst van Internet is er al snel de vraag of er nu niet gewoon over Internet gecommuniceerd kan worden, bij voorkeur tegen lage of geen kosten. Een groot deel van alle geautomatiseerde (vee-) bedrijven heeft toegang tot Internet en wil daar uiteraard ook voor de bedrijfsvoering zo efficiënt mogelijk gebruik van maken.
Gestructureerde gegevensuitwisseling over Internet is echter bepaald niet hetzelfde als wat we al deden. We krijgen nu ineens te maken met drie hoofdaspecten :

1. **Beveiliging** (kans van onderscheppen en/of verminken berichten)
2. **Betrouwbaarheid** (komt het bericht wel – binnen een bepaalde tijd – aan?)
3. **Verantwoordelijkheid** (Internet is van niemand en niemand is dus verantwoordelijk voor het afleveren)

Daarnaast is het gebruik van een andere infrastructuur, en daarmee samengaande nieuwe technieken, aanleiding om nog eens goed te kijken naar een stuk standaardisatie waar we met alle varianten van communicatietransport (ftp, e-mail, etc) en gebruik diverse syntaxen mee uit de voeten kunnen.

In opdracht van de EDI-Agro Vereniging (EAV) heeft een werkgroep zich gebogen over een aantal technische aspecten rondom het gebruik van EDI en Internet. Organisaties die in de werkgroep zitting hadden zijn allen actief op het gebied van EDI in de melkveehouderij- en/of de varkenshouderijsector. Als trekkerinstituut heeft het Praktijkonderzoek Veehouderij (afdeling Agrarische Telematica, voorheen het ATC) gefungeerd. Inzet door dit kennis- en standaardisatie-instituut is door de productschappen PZ en PVV gefinancierd vanuit het project "hergebruik en beveiliging van kritische informatie".

2 Scope en doelstelling

De werkgroep ziet het als haar opdracht om invulling te geven aan het maken van zo eenduidig mogelijke afspraken, en daar waar mogelijk te komen tot standaardisatie, rondom de volgende hoofdaspecten van electronische gegevensuitwisseling in de agrarische sector (minimaal veehouderij) in Nederland:

A. Generieke envelop

B. Beveiligingsproblematiek

C. Retourberichten

D. Huidig gebruik EDI over Internet (E-mail/FTP)

In de opdracht is nadrukkelijk niet inbegrepen een studie naar de opzet van een nieuwe EDI infrastructuur. Ook het gebruik van nieuwe EDI-syntaxen (b.v. XML) is niet de primaire doelstelling van de werkgroep geweest. Daar waar in het kader van het werken aan een duurzame oplossing nieuwe technieken of syntaxen relevant blijken is daar uiteraard wel aandacht aan besteed.

3 Groeipad EDI & Internet

De opdracht van de werkgroep was niet gelegen in een studie naar nieuwe technieken voor electronische gegevensuitwisseling, noch het opzetten van een nieuwe structuur op basis van XML. Al snel bleek echter dat bij de opzet van een duurzame, transportonafhankelijke en inhoudsonafhankelijke generieke envelop, met aandacht voor beveiliging en retourberichten, er niet om dit soort aspecten heengegaan kon worden.
In en rond het onderzoek naar de toepasbaarheid van de ebXML standaard was het een voortdurend in- en uitzoomen in de tijd. Eén van de belangrijkste bevindingen is dat er een groeipad gesignaleerd wordt voor de ontwikkeling van electronische gegevensuitwisseling over Internet. Eerst nog als huidig EDI-bericht getransporteerd over het Internet en in een laatste stadium als volwaardige e-business waarbij bedrijfsprocessen dynamisch met elkaar communiceren.

Fase	Moment	Omschrijving
0	Tot op heden	EDI (ADIS en EDIFACT) over Internet is al een feit. Er gelden echter nog amper of geen gezamenlijke afspraken over een aantal technische aspecten.
1	0-1 jaar **'korte termijn'**	Bestaande EDI-berichten worden 'gecontroleerd' over het Internet gestuurd. T.o.v. fase 0 zijn nu een aantal standaardisatieafspraken over verzending en beveiliging van toepassing. Het EDI-bericht zelf blijft ongewijzigd qua structuur en syntax. Transport vindt nu wel over Internet plaats.
2	1-3 jaar **'middellange termijn'**	Afspraken m.b.t. gebruik ebXML transport, routing en packaging module als syntax voor generieke envelop, inclusief beveiligings- en transportaspecten.
3	2-5 jaar **'lange termijn'**	ebXML als totaal framework voor alle agrarische berichtenverkeer. Gegevensuitwisseling zal zijn gebaseerd op het dynamische concept van samenwerking tussen bedrijfsprocessen. EDI is e-commerce geworden.

Figuur 1 Tijdsframe voor de ontwikkeling van gegevensuitwisseling over Internet.

N.B. fasering in tijd is globaal en puur indicatief.

De werkgroep heeft zich in haar studie gericht op fasen 1 en 2, een doorkijk naar fase 3 was echter onvermijdelijk. Nadere studie naar een eventuele invulling van het volledige ebXML concept op termijn heeft overigens niet plaatsgevonden.

Onderstaand de verwijzing van fasen naar de diverse hoofdstukken.

Fase	**Hfdst.**	**Omschrijving**
0	8	Huidige EDI-toepassingen over internet (E-mail/ftp)
1	6,7,8,9	Beveiligingsaspecten, . Retour-/ bevestigingsberichten, Huidige EDI-toepassingen over internet (E-mail/ftp), EDI-berichten via e-mail attachments
2	4, 5	Envelop, ebXML en bruikbaarheid voor agrarische edi-toepassingen
3	5	ebXML is deels bestudeerd, aspecten ervan zijn terug te vinden in hoofdstuk 5 (ebXML en bruikbaarheid voor agrarische edi-toepassingen)

Figuur 2 Fasen en verwijzing naar hoofdstukken

4 Envelop[1]

Inzet is de definitie van één generieke standaard envelop welke geschikt is voor het gebruik binnen alle veehouderijsectoren, voor zowel bestaande EDI toepassingen als ook nieuwe EDI-applicaties.

4.1 Uitgangspunten definitie en afspraken Envelop

a. **Onafhankelijk van techniek**
De envelop zal (zo veel als mogelijk) onafhankelijk gedefinieerd zijn van de te gebruiken EDI-standaard, syntax en transportmedium. Dus te gebruiken voor ADIS, EDIFACT, ascii-files, maar ook voor e-mail, traditionele EDI, FTP en XML.

b. **Opbouw volgens XML-syntax**
De envelop kent bij voorkeur een opbouw volgens de XML-standaard zodat deze door alle partijen, applicaties en verwerkingsprocedures te lezen is maar tevens is voorbereid op de nabije toekomst wanneer EDI/XML zal worden geïntroduceerd. De uitwerking zal in de vorm van een DTD-file (Document Type Definition) of Data Schema worden gedaan.

c. **Batch-gewijze gegevensuitwisseling en verwerking**
Specificaties zullen vooral gericht zijn op batch-gewijze verwerking van berichtenverkeer. Real-time verwerking wordt hiermee overigens niet buiten de scope van de werkgroep geplaatst

d. **Gebruik bestaande standaard of protocollen**
Uitgangspunt bij het ontwikkelen van technische specificaties moet zijn dat maximaal gebruik wordt gemaakt van, of aangesloten wordt bij, bestaande protocollen en internationale standaards (RFC's en REC's).

4.2 Functionele eisen

Voor de beschrijving van een standaard bericht-envelop, geschikt voor transport over Internet, is het van belang dat duidelijk is welke functionele eisen aan deze envelop moeten worden gesteld. Hierbij wordt ook gekeken naar de specifieke aspecten die gelden voor transport in een internetomgeving, waarbij er dus (extra) aandacht moet zijn voor zaken als retourmeldingen, beveiliging, etc.
De envelop moet voldoen aan de volgende functionele eisen of voorzien in de afhandeling daarvan:

1. Ontvangstbevestiging
2. Bevestiging/retourmelding van verwerking (op berichtsessieniveau)
3. Beschrijving standaard envelop; onafhankelijk van verzonden inhoud
4. Ondersteunen verschillende bestandstypen en syntaxen, ook in één bericht (b.v. ADIS, EDIFACT, etc. in één bericht)
5. Beschrijving standaard envelop; onafhankelijk van transportlaag
6. Tijdigheid; is het bericht binnen een bepaalde tijd binnen
7. Eenduidige definities in headers
8. Niet mogen inzien of wijzigen van verstuurde berichten
9. Afzender moet zijn wie hij zegt dat hij is (authenticatie)
10. Verzender moet geautoriseerd zijn om berichten te versturen (voorkomen dat iedereen kan gaan sturen, o.a. ter voorkoming crimineel gebruik)
11. Doorroutering met één of meer tussenstations, al dan niet met of zonder tussenbewerking
12. Bericht bestemd voor meerdere eindstations (met tussenstations)
13. Unieke bedrijfs-identificatie
    Als wezenlijk onderdeel van de envelop wordt een unieke bedrijfsidentificatie beschouwd. Op dit moment is hierover weinig eenduidigheid te bespeuren.

Buiten beschouwing worden gelaten:

[1] de Engelse term is Envelope, in het Nederlands wordt geschreven Envelop of Enveloppe. In dit document wordt consequent de korte Nederlandse schrijfwijze toegepast.

1. Wie mogen jouw gegevens ontvangen? Registratie van wie welke gegevens mag inzien e.d. (vastleggen intellectueel eigendomsrecht)
   Is gesteld als zijnde een discussie die in een ander platform thuis hoort.
2. Invulling eenduidige bedrijfs-id
   Alhoewel dit punt als zeer wezenlijk wordt beschouwd ziet de werkgroep het echter niet als haar taak om aan de invulling ervan (de inhoud) een oplossing te bieden.

4.3 Huidige situatie

4.3.1 Algemeen

Geschiedenis
In eerste instantie had elk EDI berichttype in de agrarische sector zijn eigen berichtheader. Zolang een applicatie alleen berichten van één berichttype ontvangt levert dit weinig problemen op. Zodra men echter meerdere berichttypen automatisch wil kunnen verwerken ontstaat al gauw de behoefte om elk bericht zoveel mogelijk op dezelfde manier te kunnen afhandelen. In 1997 is dan ook door het ATC een meer algemene header (800010) voor ADIS berichten opgezet. Deze is zoveel mogelijk afgeleid van de Edifact-header omdat die header destijds **de** standaard was. Deze ADIS header is in de meeste EDI projecten opgenomen maar helaas zijn er toch weer verschillen ontstaan, met name doordat de definitie van de header niet in één overkoepelend document is opgenomen, maar in elke afzonderlijke EDI bouwhandleiding.

Nu (2001)
Momenteel zijn de X400 netwerken al deels vervangen door het Internet. Het ziet het er naar uit dat ook EDIFACT en ADIS op termijn vervangen zal worden door het op Internet populaire XML. Het is dus maar de vraag of het nog zin heeft om te streven naar een éénduidige beschrijving van de ADIS header. In dit kader is, met de funktionele eisen en vertrekpunten in het achterhoofd, ook gekeken naar enveloperingstechnieken welke als standaard beschikbaar zijn op of rond het Internet. Omdat de ebXML standaard in deze een heel interessante component biedt is hier apart onderzoek naar gedaan, een en ander hierover in hoofdstuk 5 (ebXML en bruikbaarheid voor agrarische edi-toepassingen).

4.3.2 Bestaande EDI-berichten

Van de volgende bestaande EDI-berichten zijn de header gegevenselementen geïnventariseerd.

Berichttype	Versie	Header
EDI-NRS	4.4	800010 ADIS Header
EDI-Zuivel	3.1	800010 ADIS Header
EDI-EMM (electr. Melkmeting)		800010 ADIS Header
I&R-Rundvee		800010 ADIS Header
EDI-Pigs (incl. EDI-dap)	2001.1	800010 ADIS Header
Standaard Koppeling Varkenshouderij	981	800010 ADIS Header
TAURUS Standaard Koppeling Rundveehouderij	3.0	201861 Header Standaardkoppeling
I&R-Varkens	991	120001 Header I&R-varkens
EDI-Slacht (varkenshouderij)	2000.1	140000 Header EDI-Slacht
EDI-KPA (Kwaliteits Project Akkerbouw)	2	800010 ADIS Header
EDI-Veevoer		Edifact
Diverse EDI-Flower / FlorEcom berichttypen		Edifact

Figuur 3 Huidige EDI-headers

In de kruistabel hierna wordt de indeling van de diverse headers aangegeven:

DD-nr	Header gegevenselement	N RS	Zuiv	Emm	Ir-R	Pigs	SKV	SKR	Ir-V	Slacht	KPA	EdiFact
000000	Aanduiding datadictionary	V	V	O	V	V	V	V	V	V	V	
201685	Datadictionary-versie	V	V	O	V	V (1)	V (1)	V	V (3)		V (1)	
800001	Berichttype	V	V	O	V	V	V		V		V	H0065
800002	Versienummer berichttype	V	V	O	V	V	V				V	H0052
800009	Releasenummer berichttype	O	V	O	O	V	O				V	H0054
800006	Beheerder berichttype	V	V	O	V	V	V				V	H0051
800007	Berichtspecificatie	V	V	O	V	O	O					H0057
190912	Versienr-autorisatie-tabel (4)								V			
150000	Soort-zender								O	V		
150001	Soort-ontvanger								O	V		
150002	Soort-bericht									V		
205012	Applicatie zender	V	V	V	V	V	V				V	B0008
205014	Versienr applicatie zender	O	O	O	O	O	O				O	
201681	Naam zender					O	O	V			V	
190913	Verzendvolgnummer (5)								V	V	V	H0070
153110	Sub-bedrijfsnummer									V		
502498	Update/complete dataset										V	
B0035	Test indicator											O
202237	Nummer-bron	O	O	O	O							
190111	Verslagperiode van					O	O			V		
190112	Verslagperiode tot/met					O	O			V		
120202	UBN-melder								O			
120236	Eerste meldingvolgnummer								V			
120237	Laatste meldingvolgnr								V			
120238	Aantal verplaatsingsmeld.								C			
150004	Id-handelaar									V		
150005	id-varkenshouder									V		
201577	Systeemstatus							V				
502012	Type procescomputer							V				
201684	Versienummer produkt							V				
860141	Teeltseizoen										V	
800004	bericht id	V	V	O	V	V	V				V	H0062
201575	Bestandsdatum	V	V	O	V	V (2)	V (2)	V	V (2)	V (2)	V (2)	B0017
201576	Bestandstijd	V	V	O	V	O	O	V	V		O	B0018
205003	zender id.	V	V	O	V	V	V				V	B0004
204220	Type zender-id	V	O	O	O						V	B0007
205004	ontvanger id.	V	V	O	V	V	V				V	B0010
204221	Type ontvanger-id	V	O	O	O						V	B0007
205006	applicatie ontvanger	O	O	O	O	O	V					B0014
203984	Ind-ontvangst-bevestiging	O	O	O	O							B0031
860090	Referentie berichtId										C	
B0001	Syntax identifier (char. set)											V
B0002	Syntax version number											V
B0020	Interchange control ref.											V
B0026	Application reference											O
B0032	Communication agreement											O
B0025	Recipient ref/psw qualifier											O
202852	Legaliteitscode	O	O	O								
800008	Eventteller	O	O	O	O	O	O					T0074
203881	Pincode	O	O	O	O							
860077	Wachtwoord										V	B0022
860075	Retour-medium										O	
860076	Retour-adres										O	
205015	versienr applicatie ontv.	O	O	O	O	O	O					
153010	Applicatie			O								
201682	Naam ontvanger							O				
190104	Naam verwerkingsbureau					O	O					
150900	key-header									V		
120243	Certificeringscode software								C			
B0029	Processing priority code											O
H0068	Common access reference											O
H0073	First/last message ind.											O

Figuur 4 Header gegevenselementen per berichttype

1) Heeft als DD-nr 800003
2) Heeft als DD-nr 150800
3) Heeft als DD-nr 190911
4) Vergelijkbaar met 800002 versienummer berichttype
5) Vergelijkbaar met 800004 bericht id, maar de laatste is niet altijd een volgnummer.

In de kruistabel zijn de volgende codes gebruikt:
V Verplicht element
O Optioneel element
C Conditioneel element

De EDIFACT gegevenselementen zijn aangeduid met de code XYYYY waarbij X staat het segment aanduid (B=UNB, H=UNH, T=UNT, Z=UNZ) en YYYY het element. Andere EDIFACT segmenten (die hier niet genoemd zijn) kunnen ook relevant zijn voor het afhandelen van de diverse verschillende berichttypen zoals de segmenten BGM en RFF. Met name deze laatsten zijn vaak berichttype specifiek.

Bovenstaande lijst is niet compleet omdat bij enkele berichttypen verschillende elementen in de header voorkomen die als bericht inhoudelijk aangemerkt kunnen worden en die specifiek zijn voor een bepaald berichttype.

Voor de TAURUS Standaard Koppeling Rundveehouderij zijn dat:

201843	Max zendernummer
201844	Max koenummer
201845	Max aantal koeien
201846	Max groepsnummer
201580	Starttijd voercyclus
201579	Voercyclus
201847	Max aantal voersoorten
201848	Max voersoorten melkstal

Figuur 5 HeaderelementenTAURUS standaard

Voor EDI-Slacht zijn dat:

153109	groep-elementen (6) (7)
152301	Valuta
152302	Factor
152303	Koers
152461	BTW tarief-categorie (7)
152462	BTW percentage (7)

Figuur 6 Headerelementen TAURUS standaard

6) Wordt gebruikt om velden te groeperen.
7) Komt herhaald in de gebeurtenis voor.
Bij beide berichttypen zijn al deze elementen verplicht.

4.3.3 Netwerk envelop

Voor de afhandeling van een bericht zijn in de huidige situatie soms ook gegevens nodig uit de netwerk envelop:

From-Id	Postbusnr afzender
To-Id	Postbusnr ontvanger
Subject	Onderwerp
Filetype	Applicatieid ontvanger

Figuur 7 Netwerkenvelop

Het postbusnr van de afzender is belangrijk als in de ontvangende berichten geen unieke identificatie of geen berichttype onafhankelijke identificatie van de afzender is opgenomen.
Het filetype is in Agrotel opgenomen om op een eenvoudige manier verschillende applicaties gebruik te laten maken van dezelfde postbus.

4.4 ebXML envelop

Het streven naar een toekomstgerichte oplossing leidde al spoedig naar de standaard ebXML. Deze standaard lijkt een antwoord te bieden op de genoemde eisen als een transport- en inhoudsonafhankelijke oplossing, extra eisen m.b.t beveiliging en de voorkeur voor een envelop in XML-formaat. ebXML is ontwikkeld door de

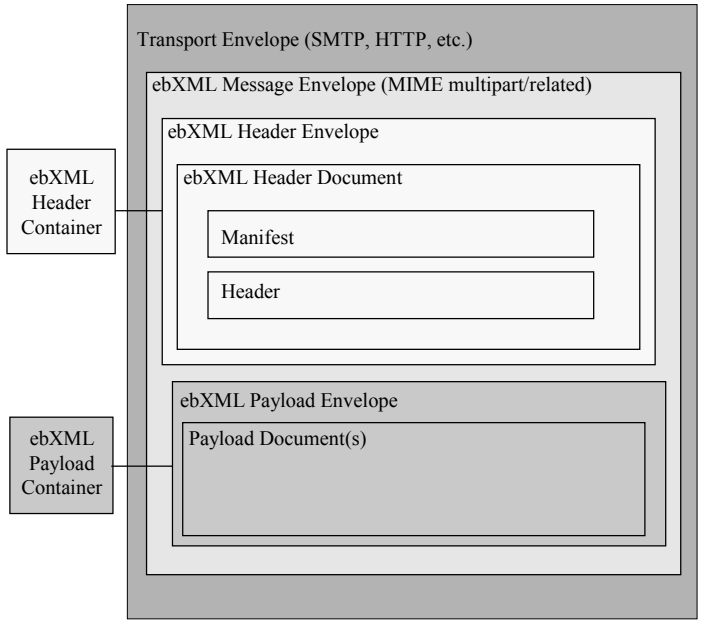
organisaties UN/CEFACT en OASIS, waarbij het ontwikkelproces is ondersteund door een groot aantal andere partijen.
De sinds mei 2001 geaccordeerde standaard lijkt een robuuste en breed gedragen standaard te worden voor het bedrijven van veilige en consistente vormen van electronische handel over Internet (dus ook EDI).

De component Transport, Routing and Packaging (TRP) beschrijft een envelop met de volgende structuur.

Transport Protocol Envelope (http, ftp, smtp)

- Message envelope (SOAP with attachments MIME envelope)
  - Header container als envelop van het headerdocument (incl. routingheader)
  - Payload met eigenlijke inhoud

En in volledig schematische weergave:



Figuur 8 EbXML envelopstructuur

De werkgroep EDI & Internet heeft een subcommissie gevraagd om de bruikbaarheid van ebXML voor de agrarische EDI-toepassingen te bestuderen.

Omdat ebXML een concept op zich is wordt deze standaard, en haar bruikbaarheid voor de agrarische EDI-toepassingen, kort besproken in het volgende hoofdstuk.

5 ebXML en bruikbaarheid voor agrarische edi-toepassingen

In dit hoofdstuk wordt in het kort nader ingegaan op een detailstudie naar de bruikbaarheid van de ebXML standaard. De studieresultaten, tezamen met de bevindingen en conclusies, zijn opgetekend in een apart rapport met de titel ***'Bruikbaarheid ebXML in agrarische EDI-toepassingen'*** en subtitel *'Studie naar de ontwikkeling van een generieke EDI-envelop (standaard) in een internetomgeving'*.
De insteek was te kijken naar de bruikbaarheid van de enveloperingstechniek en niet zozeer naar de XML-implementatie op zich, alhoewel deze zaken niet geheel los van elkaar staan. Het rapport, waarin een en ander in detail en in samenhang wordt beschreven, maakt als bijlage een integraal onderdeel uit van de totaalrapportage door de werkgroep.

Allereerst wordt een nadere uitleg van de standaard gegeven, gevolgd door een beschrijving van de mogelijkheden voor de agrarische sector en vervolgens worden de conclusies en aanbevelingen in het rapport genoemd.

5.1 ebXML standaard

De ebXML standaard bestaat uit een serie specificaties die gezamenlijk een modulair raamwerk vormen voor electronic business. De visie van ebXML is om een globale electronische marktplaats te kunnen realiseren, waarin bedrijven van elke omvang en in elke geografische locatie elkaar kunnen ontmoeten en handel kunnen bedrijven met elkaar door het uitwisselen van electronische berichten die op XML gebaseerd zijn. ebXML is een gezamenlijk initiatief van de United Nations (UN/CEFACT) en OASIS. ebXML is ontwikkeld door een wereldwijd consortium van bedrijven en is bedoeld voor wereldwijd gebruik.

In mei 2001 zijn alle specificaties afgerond en definitief geaccordeerd ('approved') als standaard.
Op dit moment zijn er reeds een groot aantal standaardisatie- en brancheorganisaties die ebXML ondersteunen en activiteiten ontplooien voor praktische invullingen. De belangrijkste ecommerce- en standaardisatieorganisatie in Nederland, respectievelijk ECP-Nederland en EAN Nederland, hebben zich ook volledig achter deze nieuwe standaard geschaard en beschouwen deze als hèt meest waarschijnlijke raamwerk voor e-business in de (nabije) toekomst, ofwel de EDI infrastructuur van morgen.
Inmiddels zijn er ook een aantal leveranciers van e-business-software die werken aan ebXML tools of aan ondersteuning daarvoor. De eerste versies en demo's zien nu het licht.

5.1.1 ebXML concept

De ebXML standaard definieert een raamwerk voor het bedrijven van collaborative-commerce (op samenwerking gerichte e-commerce). Basis is niet de gegevensuitwisseling op zich, maar meer het matchen van bedrijfsprocessen, waarbij deze processen op het niveau van informatiemodellen zijn beschreven in metataal. Bedrijven leggen vast op welke manier ze kunnen communiceren en op welke (delen van hun processen) ze willen samenwerken c.q. gegevens willen uitwisselen of delen. Door middel van zogenaamde partner overeenkomsten (CPA= Collaborative Partner Agreement) wordt vervolgens vastgelegd hoe er exact gecommuniceerd gaat worden.
Beschrijving en ook gegevensuitwisseling vindt plaats op basis van de XML-syntax, in dit geval volgens de ebXML specificaties.

In het genoemde totaalrapport is het concept van ebXML verder in detail omschreven, met daarbij ook een aansprekend voorbeeld hoe e.e.a. er bijvoorbeeld voor het bedrijfsproces Identificatie en Registratie van Runderen uit zou kunnen zien.

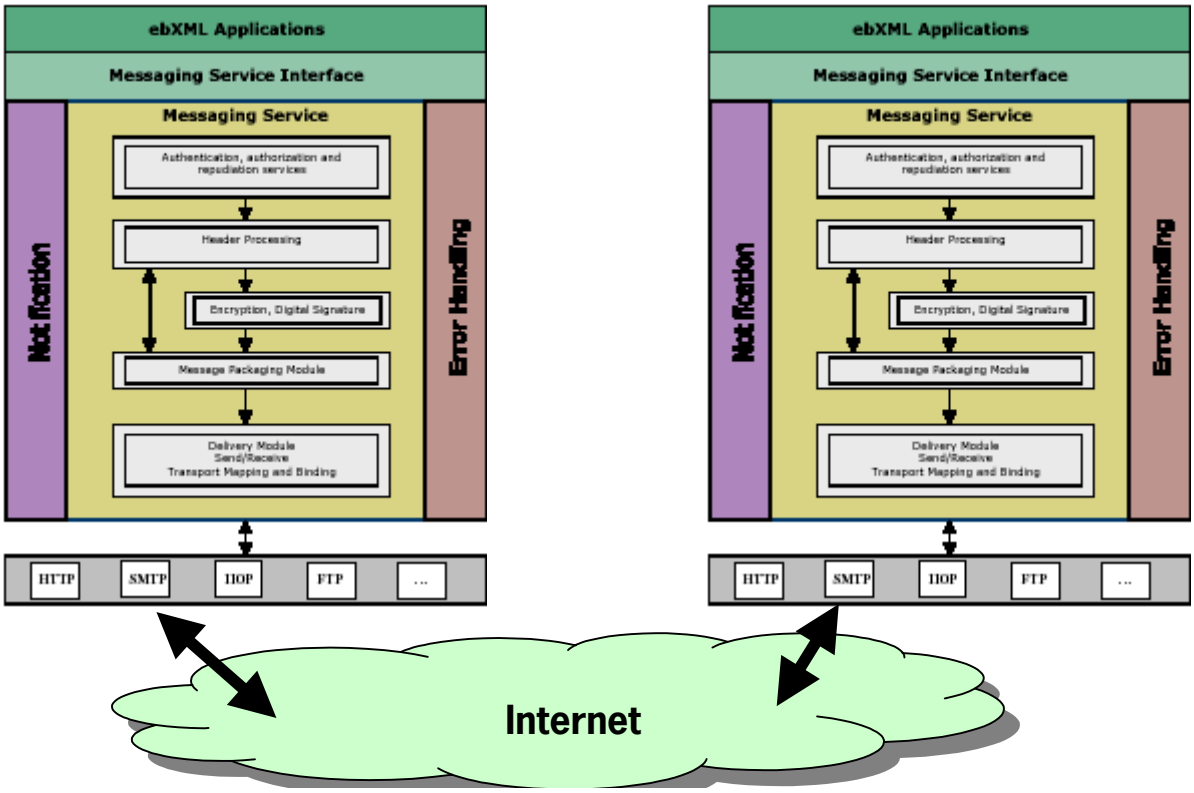
5.1.2 ebXML berichtenstructuur (Message Service Structure)

ebXML is opgebouwd uit een aantal componenten. Eén daarvan is de component 'Transport, Routing & Packaging' waarin is beschreven hoe op transparante manier niet alleen ebXML maar ook andersoortige informatie getransporteerd en verwerkt kan worden. Dit biedt bijvoorbeeld de volgende mogelijkheden:

- Verzenden van berichten over SMTP, HTTP, FTP, IIOP.

- Verzenden van verschillende soorten content (tekst, ADIS, Edifact, Video, ebXML etc.) binnen één ebXML envelop.
- Afhandeling beveiligingsaspecten zoals authenticatie, integriteit, autorisatie en de vertrouwelijkheid.

Voor de afhandeling van bovengenoemde zaken is er een Message Service Handler architectuur. Onderstaand wordt duidelijk hoe dit er schematisch uitziet.



Figuur 9 ebXML berichtenstructuur

5.2 Toepassing in agrarische sector

In de studie naar ebXML is gekeken naar de mogelijkheid voor het toepassen van een generieke envelop (incl. aspecten retourberichten en beveiliging) in de agrarische sector. Een belangrijk onderdeel daarbij is de mapping c.q. migratie van de huidige envelopstructuur naar een nieuwe.

5.2.1 Dilemma

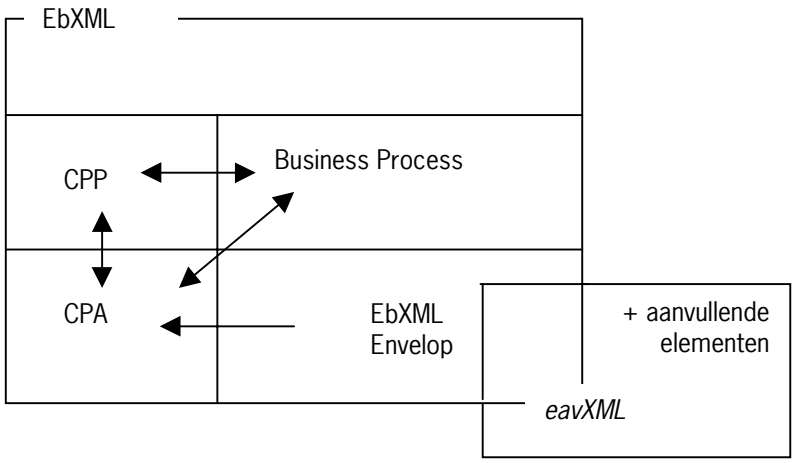
EbXML is een allesomvattende standaard voor het geheel van het bedrijven van electronische handel. EbXML is veel meer dan alleen een syntax (zoals XML op zich dat is) voor electronische uitwisseling van gestructureerde data, het begeeft zich op een niveau hoger, dat van het business proces model. Met name is gekeken naar een beperkt aantal deelaspecten van de standaard, met name rondom de component 'routing, packaging & transport'. Op het eerste gezicht een heel bruikbaar component welke echter nauwelijks los is te zien van het grote geheel.
Bij de uitwerking van de noodzakelijke elementen in de envelop, zeg maar de mapping van oude naar nieuwe elementen en de toevoeging van extra elementen vanwege nieuwe functionele eisen, komt al gauw een dilemma om de hoek kijken:

het volgen van (meer componenten) van de ebXML standaard

versus

het volgen van de ebXML standaard met (ontwikkeling) aanvullende elementen,
'de eigen ebXML variant', hierna te noemen als eavXML

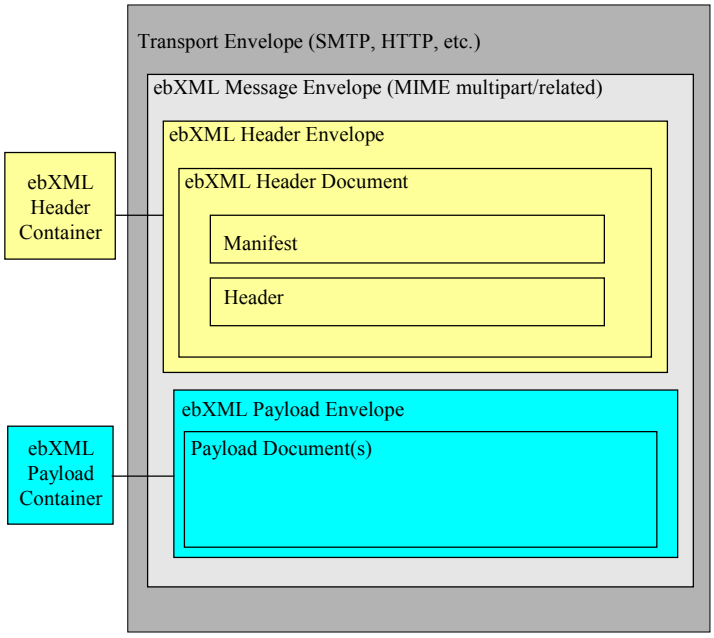
Allereerst moet worden gesteld dat niet alle (oude) elementen een plaats kunnen vinden in de ebXML standaard. Om toch invulling te geven aan een correcte en volledige envelop zullen eigen elementen moeten worden toegevoegd. Alhoewel dit mogelijk is wordt hiermee eigenlijk per direct een eigen variant van de ebXML standaard gecreëerd, gemakshalve noemen we deze de eavXML standaard . Voor een optimaal en efficiënt gebruik van de te benoemen elementen binnen de standaard zou gebruik moeten worden gemaakt van meer componenten van de standaard.
Schematisch ziet e.e.a. er als volgt uit:



Alhoewel het niet wenselijk is een eigen variant te ontwikkelen op de ebXML standaard lijkt het daarentegen op dit moment niet opportuun om meer componenten van de standaard in te zetten.

5.2.2 Basis ebXML envelop

De ebXML envelop bestaat uit een XML-bericht verpakt in een MIME-bericht. Het bevat gegevens over te versturen data (bijv. één of meer EDI-berichten), die meestal in het MIME-bericht zijn bijgesloten maar die ook afzonderlijk verstuurd kunnen worden.



Figuur 10 ebXML envelop

Op pagina 58 (bijlage EbXML: uitwerking voor agrarische EDI-toepassingen) is een praktisch voorbeeld van een ebXML envelop nader uitgewerkt, op basis van de huidige EDI-NRS header. De envelop is bewust zo eenvoudig mogelijk gehouden. In de volgende paragrafen komen mogelijke uitbreidingen aan bod.

Hier blijkt al dat de envelop tot op zekere hoogte goed bruikbaar is.

Kijken we naar de inhoud van de huidige headers dan blijkt de ebXML-envelop in hoge mate bruikbaar te zijn, als we uitgaan van een soepele migratie van de huidige naar de nieuwe omgeving.

DD-nr	Naam header gegevenselement	Mapping naar ebXML	V/O/C	Cat
000000	Aanduiding datadictionary	Kan vervallen, vermelden berichttype + versienr is voldoende.		A
201685	Datadictionary-versie	Idem		A
800001	Berichttype	Komt functioneel overeen met: <eb:Schema location="…" version="…"/>	O	A
800002	versienummer berichttype	Is attribuut 'version' in element 'Schema'	O	A
800009	Releasenummer berichttype	Kan vervallen, vermelden berichttype + versienr is voldoende.		A
800006	Beheerder berichttype	Idem		A
800007	berichtspecificatie	Idem		A
150000	soort-zender	Kan vervallen (mits zender en ontvanger elkaar kennen)		A
150001	soort-ontvanger	Kan vervallen (mits zender en ontvanger elkaar kennen)		A
150002	soort-bericht	Kan vervallen, vermelden berichttype + versienr is voldoende.		A
800004	bericht id	<eb:MessageData> <eb:MessageId> … Mits er maar 1 att. is per envelop!	V	E
201575	Bestandsdatum	<eb:MessageData> <eb:Timestamp> …	O	E
201576	Bestandstijd	Zie Timestamp		E
205003	zender id.	<eb:from> <eb:PartyId> …	V	E
204220	Type zender-id	<eb:from> <eb:PartyId type="…">	C	E
205004	Ontvanger id.	<eb:to> <eb:PartyId> …	V	E
204221	Type ontvanger-id	<eb:to> <eb:PartyId type="…">	C	E
205006	applicatie ontvanger	<eb:Service type="APPLICAT">….</eb:Service>	V	E
203984	Ind-ontvangst-bevestiging	<eb:QualityOfServiceInfo eb:deliveryReceiptRequested="…">	O	E
860090	Referentie berichtId	<eb:MessageData> <eb:RefToMessageId> …	C	E
B0001	Syntax identifier (character set)	Content-Type: text/xml; charset="…" Of <?xml version="1.0" encoding="…" ?> Indien beide opgenomen dan moeten ze gelijk zijn.	O ?	E
B0002	Syntax version number	Een characterset in ebXML heeft geen versienr.		E
B0020	Interchange control reference	<eb:MessageData> <eb:MessageId> …	V	E
B0026	Application reference	Zie applicatie ontvanger		E
B0032	Communication agreement	<eb:CPAId> …	V	E
B0025	Recipient's ref./passw.qualifier	Zie Wachtwoord.		Ea
202852	Legaliteitscode	Zie Wachtwoord.		Eb
800008	Eventteller	Kan nu gebruikt worden om te controleren of alle data-regels zijn ontvangen. Als in de ebXML-envelop deliverySemantics="OnceAndOnlyOnce" is opgegeven dan moet de MSH reliableMessagingMethod ondersteunen (of anders een foutcode teruggeven). Zie ook volgende paragraaf.		Eb
203881	Pincode	Zie Wachtwoord.		Eb
860077	Wachtwoord	In een ebXML-envelop kan een digitale handtekening worden opgenomen. Zie volgende paragraaf.		Eb
860075	Retour-medium	Zie Retour-adres.		En
860076	Retour-adres	In ebXML legt men in het autorisatiecontract (CPP/CPA) vast hoe de berichtenstroom moet lopen. Eventueel kan men in de MIME-envelop een 'Reply-To:' opnemen maar een MSH mag dit negeren.		En

Figuur 11 Relatie tussen de bestaande header gegevenselementen en de ebXML-envelop

V/O/C = Verplicht/Optioneel/Conditioneel

Categoriën:

A Autorisatiegegeven: vaste instellingen voor een bepaalde gegevensuitwisseling die men onderling of in het betreffende EDI-project zijn overeengekomen, zoals berichttype en te gebruiken datadictionary. Hoort thuis in de bericht-header/envelop of (zoals in ebXML) in een uitwisselingsovereenkomst.

E Bericht gegeven dat ook standaard voorkomt in ebXML.

Eb Bericht gegeven met een beveiligingsaspect dat door ebXML wordt afgedekt.

En Bericht gegeven uit de netwerk-envelop (MIME) van ebXML.

B Bericht gegeven: algemeen bericht gegeven, is berichttype onafhankelijk en hoort dus thuis in de bericht-header maar is niet standaard opgenomen in ebXML.

BS Berichttype specifiek gegeven: hoort dus niet in een algemene bericht-header/envelop.

X Bericht gegevens die in principe niet meer nodig of dubbel zijn.

In bovenstaand overzicht zijn alleen de header gegevenselementen uit categorie A en E opgenomen omdat die evt. vervangen kunnen worden door ebXML-envelop elementen. De overige elementen moeten in de bericht-header blijven (of kunnen zelfs geheel vervallen). Zie ook de figuur op pagina 60 (Bijlage EbXML: uitwerking voor agrarische EDI-toepassingen)

5.2.3 Aanvullende elementen

Met de beschreven basis ebXML-envelop is aan een aantal van de gestelde functionele eisen voldaan, te weten:
- Generiek
- Toe te passen in een internetinfrastructuur.
- Onafhankelijk van het gebruikte transportprotocol.
- Onafhankelijk van de te transporteren syntax.

Met name diverse beveiligingsaspecten kan men nog in deze basis envelop opnemen: fout- en retourberichten, authenticatie, autorisatie, encryptie. In de bijlage worden de verschillende ebXML elementen genoemd die hiermee te maken hebben.

5.2.4 Tools

Als we veronderstellen dat ebXML een breed gedragen standaard voor electronic business gaat worden, kunnen we ook aannemen dat er een ruime hoeveelheid tools en componenten op de markt zal gaan komen om de ebXML standaard mee te ondersteunen. In dat licht bezien is een korte onderzoek gedaan naar de beschikbare tools en componenten. Een en ander is na te lezen in het volledige rapport van de onderzoekscommissie.
Voor de laatste stand van zaken wordt verwezen naar www.ebxml.org .

Gekeken is naar tools die zelfstandig of in samenwerking met andere tools of componenten een message service handler (MSH) kunnen vormen.
Bij het zoeken naar tools is een onderscheid te maken naar de volgende categorieën of deelgebieden:
1. Complete suites
2. Software componenten
3. Ondersteunende tools

Op dit moment zijn er nog weinig complete oplossingen om een applicatie op basis van de ebXML standaard te bouwen. Naast een product van Bindsys mag alleen BizTalk Server zich ons inziens een volwaardige B2B suite noemen. Overigens moet worden opgemerkt dat Microsoft niet aangeeft dat het de ebXML standaard zelf implementeert of ondersteunt, wel geeft men derde partijen de ruimte om componenten daartoe te ontwikkelen.

Zelf een complete MSH bouwen is technisch goed mogelijk omdat er vele componenten beschikbaar zijn, maar is in principe af te raden vanuit tijds- en kostenoverwegingen.

5.3 Conclusies en aanbevelingen m.b.t. ebXML

De onderzoekscommissie is gekomen tot de volgende slotsom voor wat betreft de bruikbaarheid van ebXML. Voorafgaand hieraan eerst een paar kanttekeningen.

5.3.1 Kanttekeningen

Bij het bruikbaarheidsonderzoek is de commissie ebXML aangelopen tegen een aantal lastige kwesties. Voor het plaatsen van de conclusies en aanbevelingen in het juiste perspectief is het noodzakelijk de hieronder opgesomde kanttekeningen te kennen:

a. **Herijken bestaande headers**
Het opnieuw definiëren van de bestaande Edifact en ADIS header, bij implementatie van de ebXML of eavXML header heeft bewust geen aandacht gekregen. Het is aan de EDI verenigingen om uiteindelijk te besluiten of men met de nieuwe envelop aan de slag wil. In dat geval is het ook aan deze verenigingen te bepalen welke elementen van de header nog in stand worden gehouden. Voor het ondersteunen van een hybride omgeving (oud + nieuwe infrastructuur) is het zelfs te adviseren de oude headers intact te laten.

Omdat het dus niet zinvol is de huidige ADIS en EDIFACT headers nu op zijn kop te zetten, de nieuwe standaards staan immers voor de deur, is verder geen aandacht besteed aan de herijking van de huidige headers.

b. **EbXML is nog maar amper af en wordt dit wel de standaard?**
Een standaard is pas echt een standaard als deze wordt geadopteerd door een groot aantal partijen in de softwareindustrie. Het zal nog eventjes duren alvorens de ebXML standaard daadwerkelijk een praktijk standaard genoemd kan worden, daarvoor moet ze zich eerst in de praktijk bewijzen. Feit is dat de standaard per mei 2001 definitief is geworden en dat vrijwel alle partijen van belang deze standaard ondersteunen.

5.3.2 Conclusies ebXML

De ebXML commissie trekt de volgende conclusies:

I. Een generieke envelop op basis van ebXML is mogelijk.

II. Op dit moment zijn er echter nog geen of amper geschikte ebXML-tools om voldoende optimaal gebruik te maken van enerzijds de mogelijkheden van ebXML en anderzijds de vereiste functionaliteiten af te kunnen dekken .
De verwachting is dat dit nu wel snel zal veranderen.

III. Wil men toch snel aan de slag dan is er een alternatief in het ontwikkelen van een (deels) eigen variant op ebXML, in dit rapport de eavXML variant genoemd.
Voor de afhandeling van de communicatie e.a. zal dan wel een tool gebouwd moeten worden.

Ter onderbouwing van de conclusies II en III de volgende toelichting:

Dilemma: keuze tussen ebXML en eavXML
EbXML is nog amper te gebruiken door het gemis van geschikte tools. Ook zal er meer aandacht moeten worden besteed aan de inrichting en toepassing van andere ebXML componenten als CPP, CPA en het business process model.
EavXML is enkel toe te passen indien de specifieke (stuur-)elementen betekenis in het proces krijgen. Dit kan het beste gebeuren door het (gezamenlijk) ontwikkelen van een eigen EAV-tool.

Consequenties:

Bij het volgen van de ebXML standaard: 'Inrichting beheersorganisatie en –structuur'.
Deze organisatorische aspecten betreffen de inrichting van de beheersorganisatie, inclusief inrichting repository's en registry's. Deze kwestie speelt ook voor toekomstige schema's en namespaces. Daarvoor heb je ook een centrale plek nodig, al staat dit los van ebXML.

Bij verdere ontwikkeling eavXML
Nu een standaard 'eavXML' neerzetten heeft als belangrijke voordelen dat daarmee (internet) communicatieproblemen zijn opgelost en dat je elk willekeurig bestand kunt uitwisselen omdat je dan een generieke envelop hebt. Een niet gering resultaat!
Indien eavXML verder wordt opgepakt dan dient beseft te worden dat de commissie zich niet in detail gebogen over de definities (incl. format, cardinaliteiten, etc.) van de diverse envelop-elementen. Bij de verdere ontwikkeling zal dit nog moeten gebeuren middels de inrichting van XML schema('s) en namespaces.

5.3.3 Aanbevelingen van de ebXML onderzoekscommissie

A. Kies voor de ebXML standaard met alle noodzakelijke componenten indien er tijd is om te wachten op geschikte tools (naar verwachting ½ - 2 jaar, afhankelijk van de eisen).
Besteed dan nog wel aandacht aan de inrichting van CPA en CPP

of

B. Kies nu voor eavXML (eigen variant) totdat ebXML, inclusief tools, beschikbaar is. Maar bouw dan zelf gezamenlijk een tool voor verwerking.

C. Maak een proof of concept.
In de opdracht aan de commissie is gevraagd om een proof of concept te bouwen. Deze is binnen de grenzen van gestelde tijd en inspanning echter niet gerealiseerd. De commissie beveelt aan om, ter ondersteuning van het proces van verwerven van draagvlak, alsnog een proof of concept te maken en deze aan te bieden aan de eindopdrachtgever, de leden van EAV.

6 Beveiligingsaspecten

Beveiliging of informatiebeveiliging is een veelomvattend begrip. In dit hoofdstuk zal met name ingegaan worden op de beveiligingsaspecten rondom electronische gegevensuitwisseling, de bedreigingen, kwantificering en beheersing van de risico's en de mogelijke en beschikbare maatregelen of methoden.

Dit hoofdstuk heeft niet de pretentie om de beschikbare technieken te beschrijven, daarvoor is techniek te veel momentafhankelijk. Wel worden op hoofdlijnen een aantal methoden en technieken behandeld.

6.1 Vertrouwen en betrouwbaarheid

Veel in het leven draait om vertrouwen. De behoefte aan vertrouwen doet zich gevoelen in de context van allerhande, al dan niet commerciële, transacties. Op het commerciële vlak valt bijvoorbeeld te denken aan het afsluiten van een koopovereenkomst, waarbij onder andere vertrouwen in de kwaliteit van het product, de betrouwbaarheid van de verkoper, etc. Bij het verzenden van emailberichten kunnen de behoeften aan vertrouwelijkheid van de inhoud en aan zekerheid over de herkomst van het bericht een rol spelen. Ook zaken als het tijdstip waarop en de plaats waar een overeenkomst is gesloten zijn van belang voor het vaststellen van de rechtsgevolgen.

6.2 Beveiligingsmethoden

Betrouwbaarheid is een belangrijke voorwaarde voor het ontstaan van vertrouwen. Betrouwbaarheid wordt in een elektronische omgeving bereikt door het toepassen van beveiligingsmethoden. Deze methoden hebben tot doel de integriteit, beschikbaarheid en vertrouwelijkheid van de uitgewisselde informatie te bevorderen. Het is een misvatting dat in elektronische omgevingen een niveau van 'absolute betrouwbaarheid' noodzakelijk zou zijn. Afgezien van de vraag of absolute betrouwbaarheid in welke context dan ook haalbaar is, is het ook niet vereist. In veel situaties, bijvoorbeeld bij transacties met een geringe waarde, is een lager niveau van betrouwbaarheid voldoende. Er is geen reden om zonder meer in een elektronische omgeving eisen te stellen die men in een niet-elektronische omgeving niet stelt. Het gaat om het analyseren van de risico's en het afstemmen van het beveiligingsniveau daarop.

In onderstaande tabel zijn een aantal methoden genoemd welke bijdragen aan de verhoging van de betrouwbaarheid. Een indeling is gemaakt naar technische, organisatorische en juridische methoden enerzijds en uit te voeren door één partij, in gezamenlijkheid of door een externe onafhankelijke partij anderzijds.

	Technisch	**Organisatorisch**	**Juridisch**
Door één partij	▪ Fysieke firewall ▪ Logging/registratie	▪ Autorisatie (toegang) ▪ Interne systeemaudit (kwaliteitsoordeel)	▪ Verklaring van b.v. correcte omgang met privacy
Gezamenlijke afspraken	▪ Netwerkencryptie ▪ Digitale handtekening	▪ Public Key Infrastructure (PKI) ▪ TTP	▪ EDI overeenkomst
Door externe partij	▪ Standaardisatie techniek (b.v. EDI-bericht)	▪ Certificeringsinstituut ▪ Toezichthoudende TTP kamer	▪ Wetgeving (b.v. wet op computer-criminaliteit)

Figuur 12 Methoden ter verhoging van de betrouwbaarheid

6.3 Aspecten van beveiliging bij EDI-toepassingen

De anonimiteit en open (lees: onbeveiligde) structuur van het Internet brengt met zich mee dat de kans op misbruik van elektronische berichten wordt vergroot. Er bestaat daarom een behoefte aan middelen om berichten veilig en betrouwbaar te versturen via een open netwerk als Internet. Voor u als ondernemer is dit ook van belang. Als u een contract sluit via het Internet, wilt u weten met wie u communiceert (identificatie) en de zekerheid hebben dat degene met wie u communiceert ook werkelijk degene is voor wie deze zich uitgeeft (authenticatie). Daarnaast wilt u waarschijnlijk ook zeker weten dat er onderweg niet met het bericht is geknoeid (integriteit), een derde het bericht niet heeft kunnen lezen (vertrouwelijkheid) en wat het tijdstip is geweest waarop het bericht is verzonden (bron: ECP-Nederland)

Bedreigingen
Met onderstaande tabel wordt nog eens duidelijk gemaakt waarom het gebruik van internet per definitie bedreigingen met zich meebrengt. Voorheen als vanzelfsprekende maatregelen zijn immers nu ineens niet meer als vanzelf geregeld.
Nadrukkelijk dient te worden opgemerkt dat het overzicht enkel bedoeld is om een globaal beeld te schetsen van de bedreigingen. Zo is een VPN oplossing in allerlei varianten denkbaar die meer of minder een antwoord bieden op de genoemde bedreigingen. Ook het 'kale' internet is natuurlijk af te schermen door gebruik te maken van relatief éénvoudige maatregelen.

	X400 (besloten netwerk) b.v. Agrotel	**Internet via VPN** (virtual private network)	**Internet** Open netwerk, zonder extra maatregelen
Authenticatie d.m.v. wachtwoord	√	√	√
Versleuteling wachtwoord		√	
Authenticatie d.m.v. certificaten		√	
Encryptie van alle informatie (SSL)		√	
Archief centraal (notarisfunctie)	√	√	
Bekend waar mail (data) zich bevindt	√	√	
Afleverbevestiging postbus	√	√	
Ontvangstbevestiging geadresseerde	√	√	
Besloten community	√	√	

Figuur 13 EDI en bedreigingen naar infrastructuur (grove indicatie)

6.4 Beveiliging berichtenverkeer

Indien we ons beperken tot de beveiligingsaspecten van het berichtenverkeer dan zijn de volgende methoden interessant:

- ID-code check (username/password) - authenticatie
- Digitale handtekening/certificaat - authenticatie
- Ontvangstbevestiging/retourbericht
- Berichtvolgordenummering
- Logging/registratie berichten
- (Netwerk)encryptie
- Electronische notarisfunctie (TTP of CA)

Daarnaast kunnen nog de volgende veelomvattende beveiligingsconcepten genoemd worden:

- TTP
- VPN

De begrippen netwerkencryptie, TTP en VPN zijn in de bijlage “Enkele beveiligingstermen en concepten “ nader beschreven.

6.5 Risicobeheersing

EDI brengt voor de betrokken partijen risico's met zich mee met betrekking tot bijvoorbeeld de beschikbaarheid van het netwerk, de integriteit en authenticiteit van berichten, de exclusiviteit van toegang tot het netwerk en de controleerbaarheid van het berichtenverkeer.
Achteraf moet kunnen worden vastgesteld wie welke berichten op welk tijdstip heeft verzonden of ontvangen. Mochten er zich juridische problemen voordoen dan moet achteraf altijd te reconstrueren zijn hoe het berichtenverkeer heeft plaatsgevonden.
Om te komen tot een efficiënt en effectief gebruik van EDI moeten de risico's die inherent zijn aan de nieuwe manier van werken worden beheerst. Echter, het gebruik van EDI mag niet leiden tot nodeloze kostenverhogende en tijdverslindende procedures.

Vooraf regelen
De risico's van EDI en de wijze waarop de betrokken partijen hiermee om wensen te gaan dienen vooraf goed beschreven te zijn. Hierbij kunnen disciplines als beveiliging, juridische aspecten en *EDP-auditing*[2] een belangrijke bijdrage te leveren. Het pakket van technische en procedurele maatregelen dient toegesneden te zijn op de feitelijke situatie. Het heeft geen zin om ingrijpende en/of dure maatregelen te treffen tegen risico's die vrijwel nihil zijn, dergelijke risico's kunnen beter afgedekt worden middels een overeenkomst tussen de EDI-partners. Bij de beheersing van de risico's gaat het aldus om een uitgebalanceerd geheel van technische en procedurele maatregelen.

Raad voor Accreditatie
Voor wat betreft de (meest) kritische EDI-toepassing zal moeten worden voldaan aan de eisen die de *Raad voor Accreditatie*, ten aanzien van met name beveiliging en betrouwbaarheid, hieraan stelt.
Dit zijn overigens doorgaans dezelfde eisen die gesteld worden aan de papieren rapportage.

6.5.1 Risicoanalyse EDIFORUM

Op andere terreinen is er inmiddels een aantal EDI-toepassingen operationeel waaraan eveneens hoge eisen gesteld worden ten aanzien van beveiliging en betrouwbaarheid (denk aan electronische facturering, het plaatsen van orders, gegevensuitwisseling met douane).
Eind 1995 is vanuit EDIforum (de Nederlandse Edifact-organisatie, inmiddels opgegaan in ECP-Nederland) het rapport *Beheersing van Risico's bij EDI* opgeleverd, waarin uitgebreid aandacht is besteed aan deze problematiek. Voor het vervolg van deze notitie is dankbaar gebruik gemaakt van dit rapport.

Risico-analyse
Analyse van risico's omvat het inventariseren van te beveiligen objecten en/of processen, het in kaart brengen van alle denkbare bedreigingen en het inschatten van de schade die deze bedreigingen teweeg kunnen brengen. Waarbij de risico's zoveel mogelijk gekwantificeerd worden in termen van te verwachten verlies per incident.

Aandachtspunten risicoanalyse
Bij risicoanalyse van EDI-toepassingen dienen de volgende aspecten in ogenschouw genomen te worden:

1) ***integriteit***
   Dit omvat het gehele traject van gegevensuitwisseling. Nagegaan moet worden waar berichten verminkt of toegevoegd kunnen worden en waar berichten verloren kunnen gaan;
2) ***vertrouwelijkheid***
   Nagegaan moet worden waar berichten zouden kunnen worden afgetapt of in verkeerde handen zouden kunnen komen;

[2] EDP-auditing houdt zich bezig met de beoordeling van de kwaliteit van geautomatiseerde systemen, waarbij met name aandacht wordt besteed aan beveiliging en controleerbaarheid.

3) ***beschikbaarheid***
Nagegaan wordt waardoor de continuïteit van het berichtenverkeer in gevaar zou kunnen komen;

4) ***authenticatie en autorisatie***
Wat zijn de risico's dat een bericht niet afkomstig is van degene die in het bericht als verzender is vermeld;

5) ***controleerbaarheid***
Om berichtenuitwisseling controleerbaar te maken moeten inkomende en uitgaande berichten worden geregistreerd. Gekeken moet worden of de juistheid en volledigheid van de registraties in voldoende mate is gewaarborgd.

Ieder van deze aspecten vraagt om technische of organisatorische maatregelen binnen alle schakels van de gegevensuitwisselingsketen. Een en ander is als voorbeeld voor EDI-I&R aan de hand van het overzicht in de bijlage “Risicoanalyse EDIFORUM”, verder uitgewerkt.

Juridische status EDI-bericht
Een papieren document heeft een zekere juridische status en is soms zelfs vereist voor de geldigheid van rechtshandelingen. Over de juridische status van gegevens die door middel van electronische gegevensdragers is vastgelegd bestaat maar weinig regelgeving. Daarom is het zaak de onderlinge relatie tussen de uitwisselende partijen in de vorm van een *EDI-overeenkomst* (*Interchange Agreement*) vast te leggen.

Accreditatieprogramma
Voor het accreditatieprogramma dienen in ieder geval alle risico's geïnventariseerd en gekwantificeerd c.q. gekwalificeerd te worden. Voor de meest realistische risico's dienen beveiligings-maatregelen getroffen te worden om te voorkomen dat er iets verkeerd gaat. Echter, zelfs bij invoering van de meest vergaande beveiligingsmaatregelen zal er nog altijd een kleine kans bestaan dat er iets verkeerd gaat. Voor het accreditatieprogramma is dit acceptabel mits er duidelijke procedures gedefinieerd zijn om het ontstane probleem op te lossen.
In de toelichting op de matrix in de bijlage “Risicoanalyse EDIFORUM” (deel A) zijn de belangrijkste risico's voor EDI-I&R vermeld met daarbij de beveiligingsmaatregelen c.q. de procedures die beschreven moeten zijn in het geval er iets verkeerd gaat.

Kosten baten
Voor de meeste denkbare problemen zijn technische of organisatorische oplossingen door te voeren. Daarbij is het belangrijk dat het risico zo nauwkeurig mogelijk gewaardeerd wordt, zodat de baten die op dat punt te behalen zijn kunnen worden afgewogen tegen de kosten die de risico-nivellering met zich brengt.
In de bijlage “Risicoanalyse EDIFORUM”, deel B zijn de relevante maatregelen uit matrixtabel deel A samengevoegd, en kan per maatregel een indruk gekregen worden van de kosten en baten.

6.5.2 Eenvoudig model voor beveiligingsclassificatie

Als we de risicoanalyse uitwerken in termen van genoemde beveiligingsaspecten en mogelijke (technische-) beveiligingstechnieken dan moet het mogelijk zijn te komen tot een eenvoudig model voor beveiligingsclassificatie. Met behulp van dit model kan dan een ruwe maar snelle indicatie worden gegeven over de risico’s en gewenste maatregelen.
Het in eigen beheer ontworpen model mag niet anders worden beschouwd als een hulpmiddel voor een eerste ruwe indicatie. De opzet ervan is waarschijnlijk tamelijk arbitrair en zeker niet wetenschappelijk onderbouwd.

In onderstaand schema is uitgegaan van vijf categorieën van bedreigingen en een aantal maatregelen. Wordt bij een bedreiging een bovengemiddeld of hoog belang gezet dan zijn één of meer van de genoemde maatregelen ter overweging op zijn plaats. Komt het totaal aantal punten boven de 13 uit dan is ook enige vorm van het treffen van maatregelen te overwegen.

Bedreiging	**Belang (1-5)**	**Passende maatregelen,** indien nodig (> 2 punten)	**"papieren oplossing"** (als referentie)
Integriteit (kans op verminking, zoek raken)		Encryptie, logging, retourbericht, berichtvolgordenummer	Aangetekend versturen, Of tekenen voor ontvangst
Vertrouwelijkheid (kans op aftappen e.d.)		Encryptie, VPN	Op naam adresseren, gebruik codenamen
Beschikbaarheid (Continuïteit, tijdigheid)		SLA met netwerkprovider (SLA=Service Level Agreement)	Versturen met 24-uurs service, koeriersdienst
Authenticatie/autorisatie (Garantie van authentieke afzender)		Authenticatie m.b.v. Id-code of m.b.v. digitale handtekening	Origineel briefpapier met handtekening
Controleerbaarheid (Juistheid, volledigheid)		Logging, retourbericht	Dagafschrift
TOTAAL PUNTEN			

Figuur 14 eenvoudig model voor beveiligingsclassificatie

6.5.3 Risicoanalyse en classificatie als handvaten

Bedreigingen zijn maar moeilijk te kwantificeren en kwalificeren. Toch zou dat wel moeten kunnen, al was het alleen al ter verhoging van het beveiligingsbewustzijn (je risico's kennen). Tevens is het welkom de risico's enigszins te kunnen objectiveren en in relatie te kunnen brengen met de (noodzakelijk) te nemen maatregelen. Risicoanalyse en classificatiemethoden kunnen wat dat betreft te hulp komen als instrumenten ter bepaling van de noodzakelijk te nemen maatregelen. Dat beide instrumenten in dit rapport zijn behandeld heeft niet meer en minder als doel dat ze gebruikt kunnen worden als handvaten voor bepaling van de beveiligingseisen. Geadviseerd wordt om ze op deze manier ook te gebruiken.

6.6 Beveiliging door encryptie bij e-mail

Voor e-mail zijn er een tweetal gangbare beveiligingstechnieken, te weten S/MIME (Secure/MIME) en PGP/MIME (Pretty Good Privacy). Beiden maken gebruik van encryptie en (/of) signering. S/MIME en PGP gebruiken dezelfde soort beveiligingstechnologie en bieden dezelfde mate van beveiliging, maar ze zijn niet compatibel met elkaar. De keuze zal dus gebaseerd moeten worden op andere aspecten.
In de bijlage "E-mail-beveiliging met S/MIME en PGP" wordt een uitvoerige vergelijking uitgevoerd op de punten implementatie, verkrijgen en beheren van sleutelparen, ondersteunende platformen en kosten.

Beide beveiligingstechnieken hebben elk voor- en nadelen. De voordelen van S/MIME zijn dat er geen extra software geïmplementeerd hoeft te worden wanneer het emailpakket S/MIME ondersteund. Het nadeel is dat er een contract afgesloten moet worden met een TTP voor het verkrijgen van X509 certificaten waar kosten aan zijn verbonden. Het voordeel van het X509-sleutelpaar is dat het gericht is op een "business to consumer" denkwijze. Het is mogelijk dat een "vreemde partij" een E-mail stuurt en dat dit bericht gecontroleerd wordt op signering. Een voordeel van PGP zijn de in verhouding met S/MIME lagere kosten. Ook werkt PGP samen met bijna alle E-mailpakketten en is een X509 certificaat niet verplicht. De e-Business versie is een command-line operated versie. Met een command-line operated versie kan gemakkelijker een automatische verwerk omgeving gecreëerd worden. PGP is goed bruikbaar in een "business to business" situatie.

7 Retour-/ bevestigingsberichten

Retourberichten ter bevestiging worden als uiterst cruciaal beschouwd bij gegevensuitwisseling over Internet. Hiervoor zijn minimaal drie redenen aan te dragen:

1. **Ontbreken van zekerheid van communicatie over Internet**
   Communicatie via Internet kent geen protocollen of technieken voor het gegarandeerd bezorgen van berichten. Voorzover gebruik wordt gemaakt van de open infrastructuur van Internet zijn er ook geen partijen die – zonder het aanbieden van extra dienstverlening - deze garantie kunnen afgeven, er is immers niemand verantwoordelijk op het Internet.
2. **Toename belang kritische systemen**
   Eindgebruikers (o.a. veehouders) moeten er van op aan kunnen dat gegevens ook daadwerkelijk verstuurd of zelfs verwerkt zijn. In het bijzonder bedrijfskritische - of zelfs ketenkritische - systemen stellen steeds hogere eisen aan de betrouwbaarheid van gegevensuitwisseling. Steeds vaker zal daarbij de factor tijd een rol spelen.
3. **Introductie (product-)aansprakelijkheid**
   Ook in de agrarische sector zal (product-) aansprakelijkheid een belangrijk fenomeen gaan worden. Ondernemers moeten met zekerheid kunnen aantonen dat een handeling (koop of bijvoorbeeld I&R melding) gedaan is of zelfs op tijd is uitgevoerd. Met name is rondom de I&R regeling te verwachten dat de wet en regelgeving hieromtrent wordt afgedekt met juridische sancties.

7.1 Soorten retourberichten

Een aantal varianten met bijbehorende niveaus zijn denkbaar. Een volgende invulling is denkbaar:

1. **Ontvangstbevestiging**
   a) **negatieve ontvangstbevestiging;**
      Bij het niet kunnen afleveren c.q kwijtraken van bericht
      Dit type wordt nadrukkelijk beschouwd als geen onderdeel dat in het berichtenverkeer thuishoort. Afhandeling van niet te bevestigen berichten dient desgewenst afgehandeld te worden door het (management)systeem zelf.
   b) **positieve ontvangstbevestiging;** bij het afleveren

2. **Verwerkingsbevestiging**
   a) op berichtniveau verwerkt: ja/nee
   b) met vermelding statuscode zoals: goed, niet goed, foutcode x, etc.

Uitgangspunten en basiskeuzes
De volgende uitgangspunten en keuzes gelden:

1. Alle ontvangende partijen moeten in staat zijn (minimaal) een ontvangstbevestiging terug te sturen.
2. Of men inderdaad de retourmelding gebruikt moet vrij te kiezen, of zelfs in te stellen zijn, per (tussenliggende) organisatie en eventueel per veehouder. Via de autorisatie moet dit per 'klant' in te stellen zijn als ware het een klantprofiel.
3. Aanbevolen wordt om per berichttype (standaard) een default te kiezen (c.q.) in te stellen voor het wel of niet voorzien in retourberichten. Daarnaast zou per berichtsessie het ondersteunen van de bevestiging bepaald moeten kunnen worden in de enveloppe.
4. De werkgroep definieert een maximale set aan bevestigingsberichten. Het blijft aan de diverse partijen (EDI organisaties of eventueel zelfs op organisatieniveau) tot op welke diepte men hier gebruik van maakt.
5. Er kan niet oneindig gewacht moeten worden op een retourbericht omdat een probleem in de communicatie wellicht het afhandelen van de bevestiging onmogelijk maakt. De tijdsperiode die mag verstrijken alvorens het bericht als niet afgeleverd te mogen beschouwen moet bepaald worden.

7.2 Retourberichten op berichtniveau

7.2.1 Ontvangstbevestiging met EDIFACT

Voor EDIFACT berichten is hiervoor speciaal de zogenaamde APERAK message ontworpen. In de EDIFACT header wordt hiervoor de 'message type identifier ' gevuld met code 'APERAK'. APERAK staat voor "Application error and acknowledgement message". Voor nadere specificaties van dit bericht zie pagina 40 (Bijlage UN/EDIFACT APERAK MESSAGE).

7.2.2 Ontvangst- en verwerkingsbevestiging met ADIS

Eerder is door de gebruikersgroep EDI-Cow bekeken hoe een bevestigingsbericht er uit zou moeten zien. Gaan we uit van bevestiging op berichtniveau dan is deze tamelijk eenvoudig. We gaan dan uit van een nieuw ontwikkelde gebeurtenis met de naam 'Bevestiging bericht'.
Deze kent de onderstaande opbouw.

204041 Gebeurtenis Bevestiging bericht
Generieke gebeurtenis voor bevestiging van een bericht, voor zowel ontvangstbevestiging als ook een verwerkingsbevestiging, echter enkel op berichtniveau (niet op regel/recordniveau).

Cond.	204041	Gebeurtenis bevestiging bericht	For-mat	Veldl.	Reso-lutie	Waarde
-s-	204222	Datum-bevestiging	D	8	0	Ccyymmdd
-s-	204223	Tijd-bevestiging	T	6	0	Hhmmss
-s-	800004	Bericht-id	AN	14	0	Id. van het te bevestigen bericht.
-v-	XXXXXX	Soort bevestigingsbericht	N	2	0	Code soort bevestiging; 1=ontvangst, 2=verwerking
-v-	800001	Berichttype	AN	6	0	Type van het te bevestigen bericht
-v-	150800	Datum bericht	D	8	0	Datum van het te bevestigen bericht
-o-	XXXXXX	Code verwerkingstatus	N	2	0	Statuscode verwerking; alleen bij verwerking
-o-	XXXXXX	Verklaring verwerkingscode	AN	30	0	Nadere uitleg van verwerkingscode

S = sleutelelement; v= verplicht; o = optioneel

De bevestiging in zijn geheel wordt als een bericht gestuurd met minimaal de volgende gebeurtenissen:

1. **Een normale ADIS header**
   elk ADIS bericht heeft immers een header
2. **De gebeurtenis bevestiging bericht**
   Met hierin de bovengenoemde elementen. De data-elementen bericht-id, berichttype en datum bericht moeten voldoende informatie verschaffen voor een eenduidige identificatie van het te bevestigen bericht. Mocht er aanvullende informatie nodig zijn dan kan deze worden gehaald uit de oorspronkelijke header. De bevestiging is nadrukkelijk alleen op bericht-niveau, dus ongeacht of er meerdere regels/records zijn verstuurd wordt er slechts bevestigd op het bericht.
3. **Optioneel: extra gebeurtenissen** voor mee terugsturen van beperkte berichtinformatie.
   Zo is er bijvoorbeeld bij I&R-rund de behoefte aan extra informatie terug welke behoort bij de eerder gedane I&R melding. Zo kan er toch inhoudelijke statusinformatie (b.v. verwerkingsstatus) worden verstrekt op regelniveau. Uiteraard is een dergelijke gebeurtenis(sen) niet te vangen in een generieke definitie.

Oneigenlijk gebruik bevestigingsbericht
Veel van de huidige EDI standaarden beschrijven een berichtenstroom die slechts één kant op gaat. Een voorbeeld daarvan is EDI-I&R die alleen meldingen van veehouder naar het I&R verwerkingsbureau doorgeeft. Een retourbericht voor bevestiging is in feite een nieuwe berichtenstroom de andere kant op. Als snel kan de wens ontstaan om deze richting ook te benutten voor het doorgeven c.q. terugsturen van andere functionele informatie, anders dan feitelijke informatie m.b.t. de bevestiging.

Het is echter nadrukkelijk niet de bedoeling om retourberichten te misbruiken voor het doorgeven van nieuwe informatie. Zou dit overigens wel gebeuren, bedenk dan dat het welhaast onmogelijk wordt deze gegevens via een retourbericht terug te bevestigen.
Nieuwe functionaliteit in een nieuwe richting betekent dus per definitie een nieuwe berichtdefinitie, met eigen definitie van gebeurtenissen en gegevenselementen.

Wat dit punt betreft is de term retourbericht eigenlijk verwarrend, beter kan worden gesproken over een bevestigingsbericht of een retour-bevestigingsbericht.

Instellen gebruik bevestigingsbericht
Per EDI-toepassing, per klant of per bericht moet er de keuze zijn om bevestigingsberichten te gebruiken. Bij voorkeur zou dit in het bericht (header), dan wel in het klantenprofiel/de autorisatietabel, ingesteld moeten kunnen worden. Hiertoe is tot dusver nog geen geautomatiseerd mechanisme ontwikkeld.

Retourberichten op regel/recordniveau
Aangegeven is dat retourberichten op regelniveau vaak te gedetailleerd en daarom in zijn algemeenheid niet gewenst zijn. Toch is er soms behoefte aan het verstrekken van bevestigingsinformatie op recordniveau. Het is heel wel denkbaar dat bijvoorbeeld I&R-meldingen per record een terugmelding moeten krijgen om daarmee de juridische status (bewijslast) afdoende te kunnen waarborgen.
Helaas is het bijna ondoenlijk hiervoor een generiek bericht te ontwikkelen, dergelijke gegevens zijn immers altijd zeer specifiek per toepassing, en zelfs dan nog kan het gaan om zeer veel verschillende gegevensregels/records die om bevestiging vragen. Hooguit denkbaar is een methode waarbij in een generieke gebeurtenis de unieke key, of de inhoud van alle sleutelvelden, worden meegegeven als identificatie van de eerder gemelde regel. Deze methode is hier verder niet uitgewerkt.
Binnen de betreffende EDI-toepassing kunnen natuurlijk altijd specifieke bevestigingsberichten worden ontwikkeld.

8 Huidige EDI-toepassingen over internet (E-mail/ftp)

Als onderdeel van de uitwerking van de (gestandaardiseerde) technische afspraken EDI & Internet In de agrarische sector is er aandacht voor het gebruik van FTP als communicatieprotocol. Met name in de melkveehouderij zijn er reeds enkele FTP-servers actief die een deel van het EDI-verkeer voor hun rekening nemen.

Dit onderdeel beoogt de volgende zaken :

- Beschrijving en in kaart brengen van de specificaties van de huidige ftp-toepassingen.
- In beeld brengen van de (mogelijk) verschillende technische invullingen.
- Signaleren van knelpunten en hiaten.

De technische aspecten zullen met name gericht zijn op:

- Beveiligingsaspecten; gebruik authenticatie, autorisatie, encryptie, etc.
- Loggingsaspecten
- Retourberichten, etc.
- Aspecten rondom aansturing ftp-proces vanaf cliënt (gebruiksgemak, foutenreductie e.d.)

8.1 FTP (EDI-) toepassingen voor de veehouder

Onderstaand een opsomming van de belangrijkste actieve EDI-FTP toepassingen van dit moment. Dit overzicht is zeker niet volledig. Nadere beschouwing van de genoemde FTP-oplossingen treft u aan in

- FTP NRS
  - Server: ftp.nrs.nl
  - In beheer bij NRS/CR-Delta
  - Berichten vanaf NRS: EDI-NRS (o.a. melkcontrole en fokkerij)
  - Berichten naar NRS: EDI-EMM (melkmeting), EDI-I&R-rund, EDI-DHZ (KI)

- EDI-Zuivel/Zuivelnet
  - Server: ftp.zuivelnet.nl
  - In beheer bij SZI, uitvoering beheer door AgiS Automatisering.
  - Berichten vanaf Zuivel: technische en financiële gegevens; melkontvangst/verwerkingsgegevens
  - Berichten naar SZI: <geen>

- FTP-toepassingen van KI-Kampen en KI-Samen
  - Server: ftp.ki-samen.nl en ftp.ki-kampen.nl
  - In beheer bij eigen organisaties.
  - Berichten naar KI: KI-informatie

- NetKoerier van Rovecom
  Rovecom heeft een standaard communicatieprogramma gebaseerd op ftp waarmee volledig gestuurde communicatie tussen willekeurige cliënts en ftp-servers opgezet kan worden, dit inclusief opties voor beveiliging, logging e.d. Vooralsnog wordt dit produkt met name ingezet voor het verzorgen van gegevensuitwisseling tussen applicaties binnen bedrijven, maar is zeker ook geschikt voor het verzorgen van gegevensuitwisseling tussen bedrijven.

- Bestandsverdeler (bvd-server) van Agrotel
  Agrotel verzorgt veel berichtenverkeer in de agrarische sector. De zogenaamde bestandsverdeler kan het ophalen en verzenden van berichten verzorgen zonder dat dit in beginsel is gebonden aan een bepaalde infrastructuur of transportprotocol. Op dit moment worden op deze manier bijvoorbeeld landbouwweerberichten (beelden), maar ook berichten voor Opticrop en KPA (akkerbouw), gedistribueerd naar zowel gebruikers in de vertrouwde agrotel-postbusomgeving als ook naar internet-e-mail gebruikers. Technisch gezien kan men in principe ook een transparante berichtendienst verzorgen

waarbij er bijvoorbeeld uitwisseling van ftp (organisatie) naar e-mail (internet, veehouder) zou kunnen plaatsvinden.

- Overige producten
  Een aantal softwareleveranciers gebruikt toepassingsonafhankelijke maatwerk of standaardoplossingen. Zo wordt op dit moment in de varkenshouderij door softwareleveranciers of bedrijven incidenteel gebruik gemaakt van ftp als communicatieprotocol voor EDI.

8.2 E-mail toepassingen

Naast FTP wordt met name in de varkenshouderijsector gebruik gemaakt van e-mail voor het transport van EDI-berichten. Met name buitenlandse gebruikers van managementsystemen zijn gedwongen om via e-mail de EDI-berichten te versturen omdat zij niet, moeizaam of slechts op kostbare manier gebruik kunnen maken van de X400 inbelvoorzieningen in Nederland.
Buiten de veehouderij wordt er in de sierteeltsector nog structureel gebruik gemaakt van EDI via e-mail. In 1999 zijn in EDIFlower verband afspraken gemaakt over het gebruik van Florinet.com EDI-toepassingen als attachment aan e-mailberichten.

Een interessante ontwikkeling is de structurele inrichting van een EDI/E-mail omgeving voor de varkensfokkerijorganisatie Topigs. Momenteel wordt gewerkt aan de inrichting van een eigen e-mailserver. Deze e-mailserver zal speciaal dienst gaan doen als server voor de afhandeling van EDI berichten. Klanten (varkenshouders) krijgen een eigen postbus op het systeem en kunnen via de eigen internet (netwerk-)provider rechtstreeks verbinding maken met de server. Door te kiezen voor een dergelijke opzet wordt de kwaliteit, in termen als beschikbaarheid, verantwoordelijk-heden en registratie/logging, voor een groot deel in eigen hand genomen. Het proces blijft nog wel afhankelijk van de kwaliteit en beschikbaarheid van de netwerkprovider (toegang tot internet) en de (diversiteit aan) e-mail cliënts bij de veehouder. In feite is deze omgeving met een eigen e-mail server qua opzet gelijkwaardig aan die van de beschreven ftp-omgeving, waar de organisatie ook zelf een eigen (ftp-)server heeft.

8.3 Gebruik FTP vs. E-mail

In de melkveehouderijsector is FTP inmiddels gemeengoed. De varkenssector daarentegen lijkt meer gecharmeerd te zijn van e-mail (smtp) als transportmedium over het Internet.
Hieronder wordt getracht een vergelijk te maken tussen deze twee transportprotocollen.

Eigenschap	FTP	E-mail/SMTP
Gecontroleerde communicatie	+ Ja, door directe point-to-point verbinding	- Nee, door 'store and forward'-principe geen directe sturing
Routeringsfunctie	- Nee, echter wel te programmeren	+ Ja
Distributiefunctie	- Nee, echter wel te programmeren	+ Ja
Serverinvestering (kosten/kennis)	- Opbouw en beheer eigen ftp-server nodig	+ In principe geen extra server hardware of software nodig. Wel indien eisen hoog zijn!
Geautomatiseerde verwerking	+ Goed te sturen middels ftp-scripts of door het verwerkingsproces te programmeren.	- Minder gemakkelijk te automatiseren, tenzij het SMTP-proces ingeprogrammeerd wordt.
Push/pull	- Ontvanger moet altijd sessie starten	- of + verzender start sessie, ontvanger heeft daar geen invloed op
Tijdigheid	+ Door directe verbinding is een bericht vrijwel direct over te zetten	- Geen invloed op. Door afspraken (SLA) met netwerkprovider wel garanties te verkrijgen..
Beschikbaarheid	- afhankelijk van beschikbaarheid cliënt en server	+ Zo lang de internet infrastructuur beschikbaar is zal een bericht altijd verstuurd kunnen worden

Figuur 15 vergelijking eigenschappen FTP en SMTP (E-mail)

Met name vanwege de sterke routerings en distributie-eigenschappen van SMTP is dit protocol bij uitstek geschikt voor EDI-verkeer met n:n relaties. FTP is heel geschikt voor het afhandelen van n:1 relaties. Is directe sturing en controle, ook m.b.t. tijdskritische toepassingen, van wezenlijk belang dan lijkt FTP ook een beter bruikbaar protocol.
Niet onbelangrijk is te vermelden dat door de directe verbinding bij een FTP-sessie allerlei controlezaken op berichtniveau, zoals bevestigings/retourberichten, minder noodzakelijk lijken. Immers tijdens een FTP-sessie zal de programmatuur vrijwel altijd direct een mechanisme activeren om te controleren of bestanden wel goed zijn overgekomen. Dit is overigens geen standaard onderdeel van het FTP-protocol, maar zal altijd door de programmatuur, toegevoegd moeten worden.
Zonder dat dit verder onderzocht is zou het daarnaast nog zo kunnen zijn dat de investeringen voor een FTP-infrastructuur hoger uitvallen dan voor een e-mail infrastructuur. Met investering wordt dan zowel geld, kennis en beheersinspanning bedoeld.

De genoemde verschillen kunnen van diverse kanten behoorlijk gerelativeerd worden. Zo zijn FTP-modules gemakkelijk zelf te ontwikkelen, waarbij zondermeer functionaliteit als routering e.d. toegevoegd kan worden. FTP wordt op deze manier vrijwel een e-mailapplicatie. De keuze tussen ftp en e-mail zal dan ook vaak gebaseerd zijn op historische, relationele (wat gebruikt mijn omgeving) of emotionele argumenten.

9 EDI-berichten via e-mail attachments

In de agrarische sector is er behoefte aan het versturen van EDI-berichten per e-mail. Zo is EDI-verkeer van/naar het buitenland vaak moeilijk of geheel niet mogelijk via de X400 postbus. Daarnaast kunnen er overwegingen zijn om de toegang tot het EDI-verkeer laagdrempeliger te maken (bijna iedereen heeft immers al e-mail) of zijn er (mogelijk) kostentechnische of beheersmatige argumenten.
EDI via e-mail attachments is al een feit. Vaak worden deze berichten onbeschermd over het 'open' internet gestuurd of zijn er minstens geen gezamenlijke afspraken over beveiligings- of verwerkingsaspecten. Zo blijkt de opzet van automatische verwerking van e-mails al geen sinecure, als dat tussen slechts twee partijen gebeurd. Bij multilaterale gegevensuitwisseling zijn afspraken (of minimaal een aantal gebruiksregels) meer dan gewenst.

In andere branches bestaat uiteraard ook behoefte aan EDI-verkeer per e-mail en ook daar wordt de behoefte aan het maken van afspraken node gevoeld. In de sierteelt (Florinet van EDIFlower) is geregeld gebruik van E-mail voor EDI-verkeer al een paar jaar gemeengoed. EAN Nederland heeft in onderzoek recentelijk uitgezocht of EDI via e-mailattachments haalbaar is en heeft daarvoor een aantal gebruiksregels opgesteld. Voor een groot deel zijn deze onverkort over te nemen in de agrarische sector en kunnen dan bijdragen aan een eerste niveau van verantwoorde gegevensuitwisseling over internet, zonder dat de inhoud of syntax geraakt worden.
In dit hoofdstuk wordt ingegaan op de mogelijkheden en afspraken van het huidige EDI-verkeer, enkel getransporteerd over een ander transportmedium. Daar waar dit hoofdstuk uitsluitend ingaat op e-mail (SMTP) als transportmedium kunnen delen ervan ook van toepassing zijn op FTP.

9.1 Onderzoek en pilot van EAN

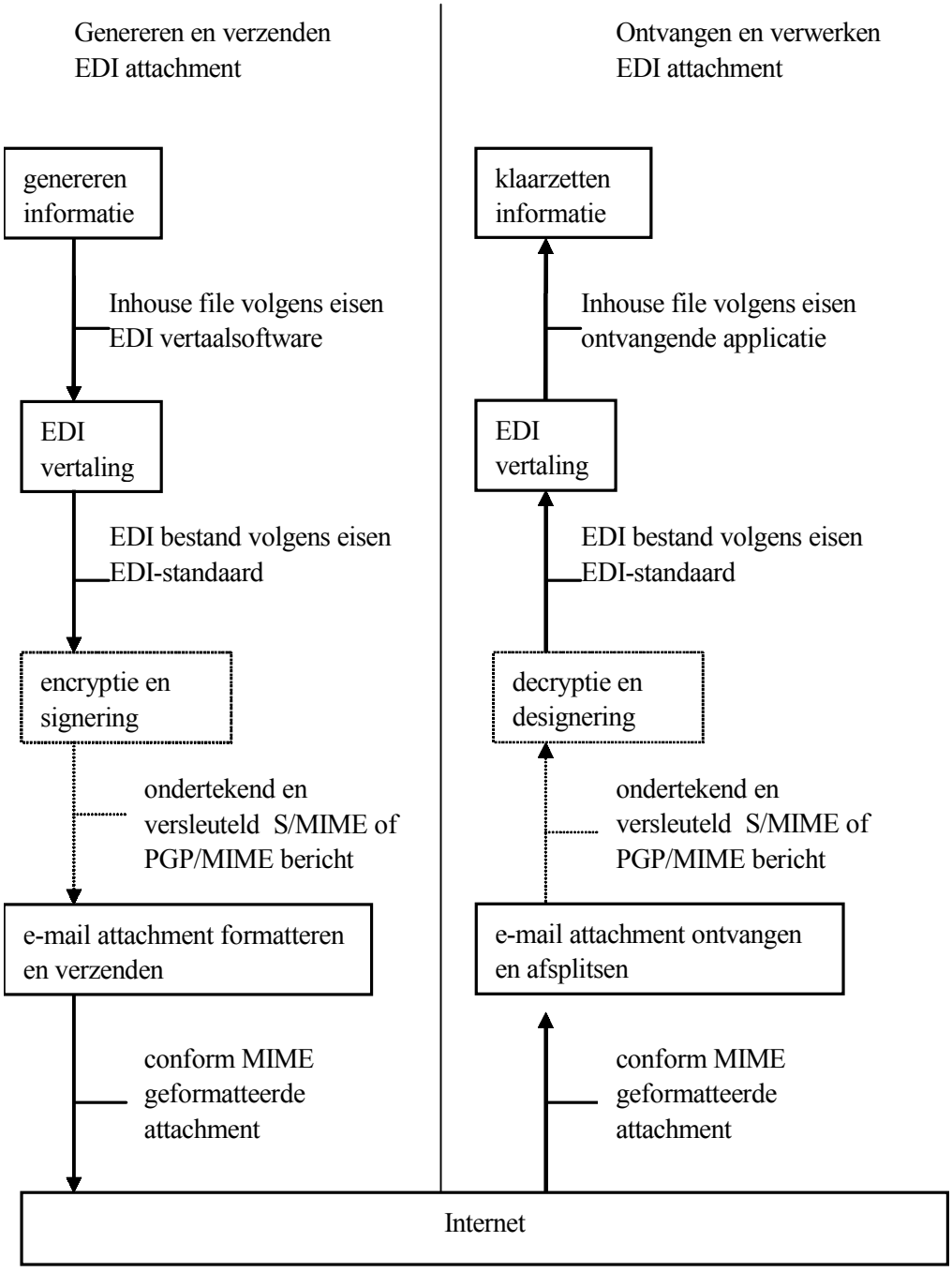
EAN Nederland heeft onderzoek gedaan en een pilot uitgevoerd naar de haalbaarheid van het versturen van EDI-berichten (EANCOM berichten in dit geval) als E-mail attachment. Gebleken is dat eventueel beveiligingsrisico's met algemeen beschikbare software kunnen worden afgedekt en dat ook de onbetrouwbaarheid van het berichtenverkeer ter hand genomen kan worden.

De pilot deelnemers komen op basis van de ervaringen tot de conclusie dat het beveiligd en geautomatiseerd versturen van EDI (EANCOM) berichten als attachment end-to-end zowel technisch als functioneel een volwaardig alternatief is voor X.400 communicatie. In bedrijfseconomische termen lijkt de haalbaarheid vooral te liggen in omgevingen waar sprake is van veel en frequent berichtenverkeer tussen goed geautomatiseerde bedrijven. Overigens wordt opgemerkt dat aspecten als het tijdkritisch karakter van de berichten en het niet kunnen aanspreken van een Internet provider bij het zoekraken van berichten in de afweging moet worden meegenomen bij het bepalen van het wel of niet gebruiken van e-mail-attachments.

EAN heeft een aantal belangrijke gebruiksregels opgesteld, waarvan de werkgroep EDI & Internet aan EAV voorstelt deze als standaard over te nemen. Daar waar de regels niet passen, of onvoldoende zijn, zijn aanvullende afspraken gemaakt.

9.2 Proces van versturen en ontvangen attachments

Onderstaand een procesoverzicht van het genereren en verwerken van een E-mail attachment



Figuur 16 Proces van vesturen en verwerken e-mail attachments

Toelichting:
In het hierboven beschreven diagram is links het proces weergegeven van het aanmaken van een beveiligd EANCOM bericht als attachment bij een E-mail bericht en rechts de verwerking ervan.. Hieronder volgt een beschrijving van de verschillende stappen.

Genereren informatie / klaarzetten informatie
Aanleveren in-house file vanuit de applicatie c.q. het klaarzetten van de gegevens voor verwerking in de applicatie

EDI vertaling
Vertalen van in-house file naar EANCOM bericht c.q. het vertalen van een EANCOM bericht naar een in-house file. Het versturen c.q. ontvangen van een EANCOM bericht als E-mail attachment stelt geen aanvullende of andere eisen aan de vertaling.

Encryptie en signering / decryptie en designering
Indien partijen dit overeenkomen kan het bericht beveiligd verstuurd worden. Het EDI bericht wordt dan bij het genereren van een beveiligde E-mail attachment door aparte encryptiesoftware versleuteld en ondertekend. Op deze manier kan het bericht niet door onbevoegden worden gelezen (versleuteling) en is bekend door welke partij het bericht wordt verstuurd (ondertekening). Eventueel kan deze stap (encryptie) volledig of gedeeltelijk worden overgeslagen afhankelijk van de eisen die aan de beveiliging van het berichtenverkeer moeten worden gesteld. Bij het verwerken van een beveiligde E-mail attachment wordt aan de hand van een vooraf ingesteld partnerprofiel of aan de hand van de meegestuurde informatie allereerst gecontroleerd of een bericht ondertekend is en vervolgens gedecrypt tot 'leesbare' informatie.

E-mail attachment formatteren en verzenden / E-mail attachment ontvangen en afsplitsen
Bij het versturen van een (versleuteld) bericht moet vervolgens de vereiste E-mail envelop worden aangemaakt en de attachment moet op de juiste manier in het E-mail bericht worden opgenomen. Bij het ontvangen van een (versleuteld) bericht moet de attachment van de rest van het E-mail bericht worden afgesplitst en klaargezet worden voor de volgende stap.

9.3 Gebruiksregels: gebruikte standaarden

De hieronder beschreven standaarden moeten zijn geïmplementeerd om het goed communiceren van EDI berichten via E-mail mogelijk te maken. Het is dus belangrijk dat softwareleveranciers deze standaarden ondersteunen. Op de website van de internet werkgroep die zich bezighoudt met EDI is hierover veel informatie te vinden (http://www.ietf.org/html.charters/ediint-charter.html). Vooral de documenten Requirements for Inter-operable Internet EDI en MIME-based Secure EDI geven een helaas technische maar wel zeer waardevolle beschrijving van de voorschriften.

Encryptie en signering

Vooralsnog zijn er alleen nog maar zogenaamde 'proposed standards' voor het ondertekenen en versleutelen van E-mail berichten. 'Proposed' in dit verband betekent dat de standaarden niet geratificeerd zijn en daarmee niet de officiële status van 'Internet standaard' bereikt hebben. De belangrijkste reden voor het niet ratificeren van de standaarden is het feit dat de standaarden gebaseerd zijn op patenten en daarmee geen volledig open standaarden zijn. Meer informatie over dit onderwerp kunt u vinden op http://www.imc.org/smime-pgpmime.html. Op dit moment liggen er twee voorstellen voor de implementatie van de beveiliging namelijk S/MIME en PGP (ook wel bekend als PGP/MIME of OpenPGP) Beiden voorstellen zijn gebaseerd op de internet Standaard RFC1847 en worden reeds in de praktijk getest.

EAN Nederland laat in haar standaards zo min mogelijk keuzemogelijkheden omdat dit de implementatie alleen maar vertraagt. Vanuit functioneel oogpunt is er geen verschil tussen PGP en S/MIME. De belangrijkste verschillen zijn de manier waarop de certificaten worden aangemaakt en de kosten. Omdat de internetgemeenschap ook nog geen keuze heeft gemaakt betekent een en ander toch dat partijen er rekening mee moeten houden dat berichten beveiligd volgens beiden formaten moeten kunnen worden verwerkt. In het hoofdstuk over beveiliging wordt in meer detail een toelichting gegeven op de zaken die spelen bij het beveiligen van berichten.

E-mail attachment formatteren en verzenden

Bij het formatteren en verzenden van E-mail attachment is vooral het correct opmaken van de E-mail envelop van belang. Uitgangspunt voor de E-mail envelop specificatie zijn de wereldwijd geaccepteerde internet standaarden welke in Requests for Comments (RFC) zijn vastgelegd. Om enige achtergronden bij deze internet standaarden te hebben wordt in deze paragraaf kort toegelicht wat er in deze RFC's wordt vastgelegd.

Van oudsher worden platte ASCII tekstberichten via het internet verstuurd. De RFC's die hierbij een rol spelen zijn RFC 821 en 822. RFC 821 definieert het transport van berichten op basis van het Simple Mail Transfer Protocol (SMTP). RFC 822 definieert de berichtrepresentatie welke in detail de 'message header' beschrijft, maar daarbij de 'message body' beschouwt als platte ASCII tekst.

Het volgens RFC 821 en 822 berichten versturen beperkt zich tot ASCII tekst (zeven bits) met een regellengte van maximaal 1000 tekens en heeft geen mechanisme voor een bericht met multimedia objecten (beelden, spraak, fax, etc.).
Genoemde beperkingen worden opgeheven door de Multipurpose Internet Mail Extensions (MIME) welke in RFC 2045 t/m 2049 zijn vastgelegd. MIME herdefinieert het formaat van de 'message body' om meerdere tekst and niet-tekst (multimedia) objecten als 'attachments' te versturen. MIME is dus een envelop waar diverse objecten in verstuurd kunnen worden. Eén van de objecten kan een EDI bericht zijn. De conventie voor het inpakken van een EDI bericht in een MIME envelop is beschreven in RFC 1767.

9.4 Aanvullende gebruiksregels en afspraken

De hieronder genoemde gebruiksregels zijn vastgesteld op basis van de ervaringen van de pilotdeelnemers tijdens de EAN pilot. De werkgroep EAV stelt voor deze regels over te nemen en deze als standaard te beschouwen. Daar waarnodig worden ze aangevuld met specifieke EAV afspraken. Een volledige lijst is weergegeven in bijlage 8.

9.4.1 E-mail envelop

Over de e-mail envelop zijn de onderstaande afspraken gemaakt. Zie vanaf pagina 65 (Bijlage Afspraken e-mail attachments (EAN + aanvullend EAV)) voor een volledig uitgewerkte overzicht.

- *Content type*
  application/EDIFACT

Aanvullend EAV: ***Content type=application/ADIS***

- *Bodypart*
  Naast de bodypart met de (beveiligde) EDI berichten geen andere type bodyparts in het bericht. 'Lege' bodyparts zijn niet toegestaan.
  Afgesproken wordt dat er per E-mail bericht slechts één attachment mag worden gestuurd.

Aanvullend EAV: meerdere berichten Meerdere berichten of bestanden zijn wel mogelijk in één gecomprimeerd bestand .

- *Content-Transfer-Encoding*
  Binaire codering: Base64

- *Subjectregel*
  Inhoud volgens bilaterale afspraken. De subjectregel mag echter niet worden gebruikt voor automatische verwerking.Hiervoor is immers de MIME Header 'content type' bedoeld. In de subjectregel kan bijvoorbeeld wel informatie t.b.v. de helpdesk worden opgenomen.

- *Naamgeving attachment*
  De naamgeving van de attachment wordt volledig vrijgelaten. Ook deze MIME header mag niet worden gebruikt om een automatische verwerking mogelijk te maken.

- *Naamgeving E-mail postbus*
  De naamgeving van de E-mail postbus is vrij te kiezen door de organisatie die de postbus aanmaakt. Geadviseerd wordt om hierbij geen persoonsnamen te gebruiken.

Aanvullend EAV: dedicated postbus Sterk aanbevolen wordt een aparte postbus te reserveren voor EDI berichten, bij voorkeur onder de bedrijfsnaam (of zoveel als mogelijk herkenbaar). Tevens wordt sterk aanbevolen enkel met positief gereputeerde internet providers zaken te doen, bij voorkeur niet de aanbieders van gratis e-mail.

- *Omvang E-mail berichten*
  Geadviseerd wordt de omvang van een E-mail bericht met een EANCOM attachment te beperken tot 2 Mb.

  Aanvullend EAV: maximale bericht omvang
  Het lijkt raadzaam de maximum grens in de praktijk, per toepasing (of b.v. gebruikersgroep) vast te stellen, de genoemde 2 Mb kan daarbij gelden als default waarde.

9.4.2 Beveiliging

Daar waar gesproken wordt over beveiliging wordt bedoeld het versleutelen van de informatie met de publieke sleutel van de ontvanger en het ondertekenen van het (versleutelde) bericht met de private sleutel van de verzender.

- *Berichten*

  Aanvullend EAV : bepaling beveiligingseisen
  Per gebruikersgroep zal bepaald moeten worden of berichten beveiligd verstuurd moeten worden. Bij het EDIFACT factuurbericht zal daar vrijwel zeker sprake van zijn.

- *Uitwisseling sleutels*
  Het uitwisselen van de sleutels kan via E-mail worden gedaan maar alleen na overleg met de ontvangende partij.

- *Naamgeving certificaat*
  Bij een sleutelpaar hoort ook altijd een certificaat. De naamgeving van dit certificaat wordt vrijgelaten.

- *Versie en sleutellengte S/MIME en PGP*
  De gebruikte beveiligingstechniek moet tenminste S/MIME v2 en PGP/MIME ondersteunen. Belangrijker is echter de sleutellengte. Vanuit beveiligingsoogpunt wordt de minimale sleutellengte vastgesteld op 1024 bits.

- *Aankomstbevestiging*
  EAN beveelt aan het EDIFACT APERAK bericht te gebruiken als ontvangstbevestiging.
  Het APERAK bericht kan worden gebruikt om de ontvangst van elk berichttype te bevestigen.
  Voor een exacte definitie van het APERAK bericht zie pagina 40 (Bijlage UN/EDIFACT APERAK MESSAGE).

  Aanvullend EAV : bevestigingsbericht in ADIS
  Omdat EAN geen ADIS berichten in beheer heeft doet zij daarover geen uitspraken. Geadviseerd wordt om voor ADIS berichten de ADIS gebeurtenis 'Bevestiging bericht' te gebruiken. Meer hierover in paragraaf 7.2.2 (Ontvangst- en verwerkingsbevestiging met ADIS).

10 Conclusies

De werkgroep EDI en Internet komt met haar studie en onderzoek tot de onderstaande conclusies.
Voor de gehanteerde fasering zie hoofdstuk 3 (Groeipad EDI & Internet).

Korte termijn

1. Uit een EAN onderzoek en pilot is gebleken dat het goed mogelijk is e-mail attachments te gebruiken voor het transport van EDI-berichten.
2. Een aantal technische gebruiksregels, grotendeels gebaseerd op EAN afspraken, kunnen als richtlijn dienen voor de invoering van een verantwoord gebruik van EDI over Internet.
3. Het is niet opportuun om voor de korte termijn een nieuwe generieke header of envelop te ontwikkelen zonder gebruik van de enveloperingsmethodiek van ebXML.
4. Met ebXML kan goed een nieuwe generieke envelop worden opgezet. Op dit moment lijkt dit praktisch echter nog niet haalbaar, tenzij ervoor gekozen wordt om zelf een tool te ontwikkelen voor de afhandeling van de berichtenstructuur.
5. In de melkveehouderij lijkt er een sterke voorkeur te zijn voor het gebruik van FTP, in de varkenshouderij gaat de voorkeur uit naar SMTP (e-mail) als transportprotocol. Bij vergelijking zijn er wel duidelijke verschillen te bespeuren, in de praktijk zal de afweging echter eerder worden gedaan op basis van argumenten die niet van functionele aard zijn.
6. Risicoanalyse en beveiligingsclassificatie zijn instrumenten die goed bruikbaar zijn bij het kwantificeren van de risico's en de bepaling van de noodzakelijk te nemen maatregelen. Voor wat betreft beveiligingsmaatregelen zijn er een aantal methoden of technieken voorhanden.

Middellange termijn

7. Voor de middellange termijn is de implementatie van de ebXML envelop interessant. De te gebruiken ebXML module (transport, routing & packaging) biedt naast ruime mogelijkheden voor het transportonafhankelijk sturen en routeren van berichten tevens de functionaliteit voor de afhandeling van beveiligingseisen en retourberichten.

Lange termijn

8. Voor de lange termijn voorziet de werkgroep een rol van betekenis weggelegd voor de ebXML standaard als volwaardig concept voor de toepassing van e-business in de agrarische sector.

11 Aanbevelingen

De werkgroep doet de volgende aanbevelingen aan haar opdrachtgever (EAV).

1. Geadviseerd wordt de opgestelde gebruiksregels voor een verantwoorde gegevensuitwisseling over internet (korte termijn) te implementeren.
2. De hulpinstrumenten risicoanalyse en beveiligingsclassificatie worden aanbevolen om gebruikt te worden bij de vaststelling van de beveiligingsrisico's i.r.t. de te nemen maatregelen.
3. Voor de implementatie van een nieuwe generieke envelop wordt geadviseerd hiervoor de betreffende module van ebXML te gebruiken zodra er voldoende bruikbare tools voorhanden zijn.
4. Mocht het wachten op de onder punt 3 bedoelde tools ongewenst zijn dan kan er voor worden gekozen om een eigen 'Message Service Handler' applicatie te bouwen voor de juiste processing van de ebXML envelop.
5. Voor de middelllange en langere termijn wordt aan EAV het advies gegeven om zich te richten (c.q. oriënteren) op implementatie van het volwaardige ebXML framework. Speciale aandacht moet daarbij uitgaan naar:
    a. Nader onderzoek en uitwerking van inrichting van de ebXML componenten CPA en CPP
    b. Maak proof of concept voor draagvlak en promotiedoeleinden
    c. Schep randvoorwaarden voor inrichting van een ebXML beheersorganisatie
    d. Schep randvoorwaarden voor de opzet of inrichting van een agrarische repository en inrichting van XML data-schemas en namespaces

Literatuur

Gehanteerde basisdocumenten

De in dit rapport gehanteerde afspraken en richtlijnen zijn gebaseerd of afgeleid van de volgende basisdocumenten c.q. standaards:

1. Rapport: **EANCOM als E-mail attachment**;
   EAN Nederland, september 2001
   Standaarden en gebruiksregels voor het geautomatiseerd communiceren van beveiligde EANCOM berichten als E-mail attachment.

2. Intern rapport: **Bruikbaarheid ebXML in agrarische EDI-toepassingen**;
   Commissie ebXML van de EAV werkgroep EDI & Internet; Oktober 2001; referentie: 013197r15 (eindredactie: Praktijkonderzoek Veehouderij)
   Studie naar de ontwikkeling van een generieke EDI-envelop (standaard) in een internetomgeving

3. Rapport: **Beheersing van risico´s bij EDI**
   EDIforum, 1999

4. EDIFACT standaard;
   Message Type : APERAK, version: D, Release: 99B,
   Contr. Agency: UN, Revision: 4, Date: 1999-09-11

Bronnen op het internet

www.abz.nl	ICT-/standaardisatie organisatie verzekeringswereld
ecommerce.internet.com	E-commerce guide op internet
www.biztalk.org	BizTalk framework
www.commerceone.com	E-marketplace en initiatiefnemer voor standaardisatie
www.ean.nl	EAN Nederland
www.ebxml.org	ebXML homesite
www.ecp.nl	E-commerce Platform Nederland (incl. oude Ediforum)
www.microsoft.com	B2B oplossingen
www.oasis-open.org	Organization for the Advancement of Structured Information Standards
www.openapplications.org	Open Applications Group (beheer aantal EDI standaards)
www.tie.nl	Commercieel e-business bedrijf; participant ebXML
www.w3.org	World Wide Web Consortium
www.xedi.org	XML-EDI oplossingen
www.xml.org	XML portaal
www.xml-edifact.org	XML-EDIFACT site
www.xmlspy.com	XML ontwikkel suite (software)
www.unece.org	United Nations Economic Commission for Europe (UN/EDIFACT)

Overige bronnen

Merkow, M. , 2001
VPN voor Dummies (Virtual Private Networks For Dummies), Addison Wesley, 320 p, ISBN 90 430 0332 8

Raman, D. , 2000
B2B eCommerce, Cyber Assisted Business in de praktijk, TIE Holding NV, 331 p., ISBN 90-805233-4-8

EDIFlower – projectgroep techniek Florinet, 1999
Technische afspraken Florinet.com, referentie: Flor-TA-V22.doc

Bijlagen hoofddeel A: diversen

Bijlage 1. Enkele beveiligingstermen en concepten

(Netwerk)encryptie
Encryptie is het verbergen of maskeren van informatie door middel van cryptografie. Encryptie is mogelijk op verschillende niveau's: op bestandsniveau, op het transportprotocol, tussen cliënt en server of tussen gebruiker en applicatie.
Secure Socket Layer is een beveiligingsprotocol dat bijvoorbeeld de authenticatie tusssen cliënt en de server regelt. Veel beveiligde web-sites (http of shhtp) gebruiken SSL.
Bij e-mail applicaties wordt vaak S/MIME (Secure/multipurpose Internet mail extensions) of PGP (Pretty Good Privacy) gebruikt als encryptietechniek. De eerstgenoemde maakt gebruik van sleutelparen waarvan de public key uitgegeven wordt door een certificaatautoriteit (CA).
Encryptie wordt ook toegepast bij Virtual Private Networks (VPN), in dat geval zijn meerdere encryptieprotocollen beschikbaar, zoals bijvoorbeeld IPSec

Digitale handtekening of certificaat
Encryptie stelt de afzender van een bericht in staat een digitale handtekening te maken. Een berichtsamenvatting wordt berekend , versleuteld met de privésleutel van de afzender en daarna aan het bericht toegevoegd. Met een digitaal certificaat wordt de algemene sleutel van een gebruiker bedoeld waarmee het bericht door de zogenaamde certificaatautoriteit wordt ondertekend.
Certificaten (digitale handtekeningen) dragen zorg voor:

- dat berichten echt van de afzender afkomstig zijn
- bescherming tegen ongewenste wijziging van het bericht
- garantie dat bericht onderweg niet is ingezien (door derden)

Trusted Third Parties (TTP) en Certificeringsautoriteit (CA)
TTPs zijn onafhankelijke organisaties die diensten aanbieden waarmee de betrouwbaarheid van elektronisch berichtenverkeer kan worden vergroot. TTPs maken gebruik van cryptografie om de authenticiteit of de vertrouwelijkheid van berichten te vergroten.
In principe zijn TTP's organisaties die diensten aan kunnen bieden op meerdere fronten ter bevordering van de betrouwbaarheid. De belangrijkste functies die men biedt zijn die van sleutelbeheer, certificeren en de bewijsfunctie. Organisaties die sleutels uitgeven, beheren en certificeren (= garanderen van binding tussen een publieke sleutel en de gebruiker van de bijbehorende privésleutel) heten ook wel een certificeringsautoriteit, ofwel een CA.
De meerwaarde van een CA is vooral gelegen in het kunnen garanderen van authenticiteit, maar zeker ook in het bieden van de bewijsfunctie. Voor de bewijsfunctie van een document is het van belang dat er garanties zijn dat de inhoud van het document ongewijzigd is. Een TTP kan hiervoor zorgen door het document bijvoorbeeld te waarmerken of door waarborgen te bieden voor de juistheid van de digitale handtekening van de maker. Voorts kan het bij geschillen noodzakelijk zijn te bewijzen dat een elektronisch bericht verzonden of ontvangen is (*non-repudiation* oftewel onloochenbaarheid). Een TTP kan onloochenbaarheid garanderen door bijvoorbeeld digitaal getekende bevestigingen te versturen van verzending en ontvangst. Tevens kunnen elektronische berichten door een TTP worden voorzien van tijdstempels (*time-stamping*). Dit kan van belang zijn om te bewijzen op welk tijdstip een bepaalde rechtshandeling heeft plaatsgevonden

In Nederland zijn notarissen, accountants, banken, telecommunicatie bedrijven en PTT Post bezig met het oprichten van TTPs. Het bekendste voorbeeld van een TTP is waarschijnlijk Verisign, een Amerikaans bedrijf dat certificaten uitgeeft waarmee e-commerce websites hun authenticiteit garanderen.

VPN
Daar waar het internet per definitie als onveilig bekend staat zijn er partijen die een beschermde eigen (private) omgeving op internet aanbieden. Via technieken als het toepassen van VPN's (Virtual Private Networking) kan dan toch veilige communicatie van en naar het 'vrije Internet' worden gegarandeerd.
Een VPN kan worden gedefinieerd als een beveiligde route voor gegevens in de vorm van een 'tunnel door Internet' die gebruik maakt van versleuteling (cryptografie) om de inhoud van de berichten te verbergen tijdens transport via algemeen toegankelijke netwerken.

Organisaties kunnen zelf VPN-oplossingen inzetten of bepaalde beveiligde berichtenverkeer laten lopen via een gespecialiseerde berichtendienstverlener (vgl. VAN, alleen nu voor Internet). In het eerstgenoemde geval zal per organisatie minimaal een kostbare architectuur met een firewall (veelal bij organisaties al aanwezig) en een tunnelserver ingericht moeten worden en zullen alle berichten communicerende computers uitgerust moeten worden met internet-tunnel-cliënt-software.
Gekozen kan worden voor een gespecialiseerde beveiligde berichtendienstverlener als er vele (EDI-) toepassingen en organisaties vragen om een beveiligingsoplossing en eigen aanschaf van hard-/software te kostbaar is of indien men een dergelijke taak liever bij een onafhankelijke partij neerlegt. De derde partij neemt a.h.w. de investering voor de hard- en software over en kan als onafhankelijke een volledige notarisfunctie (door logging, archivering e.d.) uitvoeren.

Bijlage 2. E-mail-beveiliging met S/MIME en PGP

Implementeren van S/MIME en PGP

S/MIME
Om S/MIME te implementeren is het niet nodig om software te installeren als er gebruik gemaakt wordt van een emailpakket dat S/MIME ondersteund. Wanneer hiervan geen sprake is, dient er een pakketwijziging of upgrade te worden uitgevoerd. Wanneer hiervan wel sprake is, dient er een X509 sleutelpaar bekend gemaakt te worden.

PGP
Om PGP te implementeren dient er software geïnstalleerd te worden. PGP integreert met de emailpakketten die genoemd zijn in paragraaf 0. PGP bevat een tool die een sleutelpaar kan genereren dus is het niet nodig om een X509 sleutelpaar certificaat te hebben. Een reeds verkregen X509 sleutelpaar kan echter wel worden geïmporteerd. De methode zonder het X509 sleutelpaar staat bekent als 'direct trust'. Direct trust is volledig betrouwbaar en vooral bedoeld voor omgevingen waarin de communicatiepartners elkaar kennen. Voor het importeren van de zelf gegenereerde sleutel en de sleutel van het X509 certificaat dient dezelfde werkwijze gevolgd te worden.

Het verkrijgen, beheren en controleren van sleutelparen

Het verkrijgen van een X509 sleutelpaar:
Voor het verkrijgen van een X509 sleutelpaar dient er een contract afgesloten te worden bij een Trusted Third Party (TTP). In Nederland zijn er TTP's actief. De partij die het contract afsluit wordt de administrator genoemd. De administrator moet samen met de TTP een database en een internetsite configureren. In deze database moeten de naam en adresgegevens en een wachtwoord ingevoerd worden, voor de instellingen die een sleutelpaar willen hebben. Vervolgens moeten de gegevens die ingevuld moeten worden op de aanmeldsite uitgewisseld worden. Zodra een instelling deze gegevens ontvangen heeft, kunnen deze gegevens worden ingevoerd op de aanmeldsite. Na het invullen en een akkoordbevestiging wordt er een sleutelpaar gegenereerd op de pc. De publieke sleutel wordt in de database opgeslagen. Vervolgens moet een zogenaamde administrator controleren of de gegevens van de aanvrager correct zijn. Het hangt van het soort contract af of de controle automatisch gebeurt of dat de administrator het controleren fysiek moet doen. Wanneer uit de controle blijkt dat de gegevens correct zijn, worden de gegevens doorgespeeld aan de TTP. Vervolgens wordt er een bevestiging naar de aanvrager gestuurd.

Het beheren en controleren van de S/MIME sleutels:
Bij S/MIME wordt het sleutelbeheer geregeld door een TTP. De TTP heeft van elke partij de publieke sleutel. De controle op geldigheid van het X509-sleutelpaar zal dan ook on-line plaats moeten vinden. Deze situatie is ideaal in een "business to consumer" c.q. "any to any" situatie. Elke partij kan een bericht sturen en dit bericht kan vervolgens gecontroleerd worden bij de TTP. Het is dan zeker dat dit bericht werkelijk van deze partij af komt. Het is niet duidelijk of de emailpakketten een eenmaal gecontroleerd sleutelpaar vast houd of dat deze controle iedere keer uitgevoerd moet worden.

Het beheren en controleren van de PGP sleutels:
Bij PGP ligt het sleutelbeheer in eigen hand. Er is een tabel waarin alle sleutelparen vastgelegd dienen te worden. In deze tabel worden de publieke sleutels van de afzenders vastgelegd. Aan de hand van deze tabel worden de controles op het signeren gedaan. Deze werkwijze is dus meer gericht op een "business to business" situatie. De partijen moeten elkaar kennen en de publieke sleutel moeten vooraf uitgewisseld worden. Ook moet er een goede administratie voor het beheer van de sleutels worden opgezet.

Platformen die S/MIME en PGP ondersteunen

Niet elk besturingssysteem en niet elk emailpakket ondersteunt de beveiligingstechnieken S/MIME en/of PGP. In de onderstaande tabel worden de besturingsystemen en emailpakketten genoemd die S/MIME en PGP ondersteunen voor zover op dit moment bekend. Voor S/MIME is niet duidelijk welke versies van de verschillende pakketten ondersteuning bieden en welke sleutellengte gebruikt wordt. Let erop dat in deze standaard de sleutellengte op 1024 bits wordt vastgesteld en dat dus bij aanschaf gecontroleerd moet worden of dit ondersteund wordt.

S/MIME:	
Besturingssysteem	*Emailpakket*
Windows 9*	Microsoft outlook 98 e.v.
Linux	Outlook Express *
	Netscape messenger *
	Lotus Notes *
	Eudora *
NB: van de vermeldingen met een * kon door de leveranciers geen versienummer worden opgegeven	
PGP:	
Besturingssysteem	*Emailpakket*
Windows 95b/98/ME/NT/2000	Microsoft Outlook 97
Linux	Outlook Express 4.0/5.0
Solaris	Lotus Notes 4.x/5.x
Mac	Group Wise 5.2/5.5
AIX	Eudora 4.x
S/390	Claris 2.x
Novell	Elm
	Pine, Mutt
	ICQ instant messaging

Figuur 17 Platformen die S/MIME en PGP ondersteunen

De kosten van S/MIME en PGP

S/MIME
Wanneer gebruikt gemaakt wordt van een pakket dat S/MIME ondersteunt zijn de enige kosten, de kosten van het X509 sleutelpaar. Dit zijn de kosten van het contract met de TTP. De hier onderstaande tabel is in oktober 2000 opgesteld en moet dus worden beschouwd als een indicatie. Verder kunnen de kosten per TTP verschillen. Ook bestaat de mogelijkheid om bij een bestaande TTP individuele certificaten af te nemen. Na het kostenoverzicht wordt een korte toelichting gegeven. De onderverdeling van kostenposten is aan de orde geweest bij de uitleg van het verkrijgen van een X509 sleutelpaar.

Kostenindicatie X509 Certificaten (bron KPN Telecom oktober 2000):				
	Aantal certificaten	500	1000	2500
Handmatige	1) Jaar 1	FL 12.500	FL 16.500	FL 33.500
	2) Vervolg jaren	FL 10.000	FL 14.000	FL 31.000
Geautomatiseerd	3) Jaar 1	FL 66.020	FL 70.020	FL 87.020
	4) Vervolgjaren	FL 18.920	FL 22.920	FL 39.920

Figuur 18 Kosten S/MIME en PGP

Ad 1)
De kosten hebben betrekking op de initiatie van de dienstverlening voor de klant, configuratie van de betreffende toepassing en opleiding van de beheerder.

Ad 2)
De kosten hebben betrekking op een licentie voor de software die gebruikt wordt voor het aanmelden en het registreren van de aanvragers in de database. Deze kosten zijn gekoppeld aan het aantal uit te geven certificaten. Het minimale aantal is 500.

Ad 3)
De kosten hebben betrekking op een éénmalige software licentie waarmee op een eigen webpages personen certificaat aan kunnen vragen en de aanvraag vervolgens automatisch kan worden afgehandeld. Het tarief omvat naast licenties, implementatie en training van de beheerders.

Ad 4)
De kosten hebben betrekking op onderhoud, updates en support.

PGP:
Voor PGP is het niet verplicht een X509 sleutelcertificaat te gebruiken. De kosten die beschreven staan bij S/MIME zijn dus hier optioneel. PGP biedt verschillende versies.
De standaardversie is “PGPMail and PGPfile encryption v7.0”. De kosten hiervan zijn 63 Euro voor de versie met een licentie van 2 jaar en 122 Euro voor de versie met onbeperkte licentie. Deze versie is niet command-line operated. Het voordeel van een command-line operated versie is dat deze beter geschikt is voor het geautomatiseerd verzending en ontvangen van berichten. Verder is de PGP e-Business server versie verkrijgbaar. Deze versie is wel command-line operated. De kosten hiervoor zijn 7.532 euro voor de 2 jarige licentie en 10.760 euro voor een onbeperkte licentie. Worden er meer licenties besteld dan wordt de aanschafprijs minder. Bij de 2 jarige licentie zit het recht om updates en upgrades te downloaden, toegang tot de online knowledge database te krijgen en de mogelijkheid om problemen per E-mail aan te bieden. Bij de onbeperkte licentie zitten deze opties niet. Hiervoor zijn wel contracten af te sluiten (bron: Nedsecure februari 2001).

Bijlage 3. UN/EDIFACT APERAK MESSAGE

United Nations Directories
for Electronic Data Interchange for
Administration, Commerce and Transport

UN/EDIFACT

Message Type : APERAK
Version : D
Release : 99B
Contr. Agency: UN

Revision : 4
Date : 1999-09-11

SOURCE: Joint Transport Group (JM4)

CONTENTS

Application error and acknowledgement message

For general information on UN standard message types see UN Trade Data Interchange Directory, UNTDID, Part 4, Section 2.3, UN/ECE UNSM General Introduction

---

0. INTRODUCTION

This specification provides the definition of the Application error and acknowledgement message (APERAK) to be used in Electronic Data Interchange (EDI) between trading partners involved in administration, commerce and transport.

1. SCOPE

1.1 Functional Definition

The function of this message is:
a) to inform a message issuer that his message has been received by the addressee's application and has been rejected due to errors encountered during its processing in the application.
b) to acknowledge to a message issuer the receipt of his message by the addressee's application.

1.2 Field of Application

The Application error and acknowledgement message may be used for both national and international applications. It is based on universal practice related to administration, commerce and transport, and is not dependent on the type of business or industry.

1.3 Principles

A message being first controlled at system level (CONTRL) to detect syntax errors and to acknowledge its receipt is then transmitted to the application process to be processed.

If an error is detected at the application level, which prevents its complete processing, an APERAK message is sent to the original message issuer giving details of the error(s) encountered.
If no error has been detected and when an acknowledgement is necessary (when no dedicated answer to the original message exists) an APERAK message is sent precising the reasons of acknowledgement.
In case of application error, the APERAK message will need manual processing e.g. when the underlying reason is a programming error.

In case of acknowledgement the APERAK message may be automatically or manually processed at recipient's discretion.

2. REFERENCES

See UNTDID, Part 4, Chapter 2.3 UN/ECE UNSM - General Introduction, Section 1.

3. TERMS AND DEFINITIONS

3.1 Standard terms and definitions

See UNTDID, Part 4, Chapter 2.3 UN/ECE UNSM - General Introduction, Section 2.

4. MESSAGE DEFINITION

4.1 Segment Clarification

This section should be read in conjunction with the segment table which indicates mandatory, conditional and repeating requirements.

0010 UNH, Message header
A service segment starting and uniquely identifying a message. The message type code for the Application error and acknowledgement message is APERAK.

Note: Application error and acknowledgement messages conforming to this document must contain the following data in segment UNH, composite S009:

Data element 0065 APERAK
0052 D
0054 99B
0051 UN

0020 BGM, Beginning of message
A segment to indicate the type and function of the message and to transmit the identifying number.

0030 DTM, Date/time/period
A segment to specify related date/time.

0040 FTX, Free text
A segment to specify free form or processable supplementary information related to the whole message. In computer-to-computer exchanges free form text will normally require the receiver to process this segment manually.

0050 CNT, Control total
A segment to provide message control totals.

0060 Segment group 1: DOC-DTM
A segment group to provide information on the document being acknowledged.

0070 DOC, Document/message details
A segment to provide the necessary identification information about the document being acknowledged.

0080 DTM, Date/time/period
A segment to provide the relevant dates concerning the document being acknowledged.

0090 Segment group 2: RFF-DTM
A group of segments to specify the document/message to which the current message relates, and related date and time.

0100 RFF, Reference
A segment to indicate the reference number of the document/message.

0110 DTM, Date/time/period
A segment to specify the date and time of the referenced document/message.

0120 Segment group 3: NAD-CTA-COM
A group of segments to specify the identifications of message sender and message receiver with their contacts and

communication channels.

0130 NAD, Name and address
A segment to specify the identification of the message issuer and message receiver.

0140 CTA, Contact information
A segment to specify a person or department inside the party's organization, to which communication should be directed.

0150 COM, Communication contact
A segment to indicate communication channel type and number inside the party's organization, to which communication should be directed.

0160 Segment group 4: ERC-FTX-SG5
A group of segments to identify the application error(s) within a specified received message and to give specific details related to the error type or to precise the type of acknowledgement.

0170 ERC, Application error information
A segment identifying the type of application error or acknowledgement within the referenced message.
In case of an error, the error code may specify the error in detail (e.g. a measurement relating to a piece of equipment is wrong) or as a rough indication (e.g. a measurement is wrong).

0180 FTX, Free text
A segment to provide explanation and/or supplementary information related to the specified application error or acknowledgement.
For example, the explanation may provide exact details relating to a generic error code.

0190 Segment group 5: RFF-FTX
A group of segments to specify the functional entity reference (e.g. goods item level, equipment level) relating to the specified error; further details can be added to identify the error more precisely.

0200 RFF, Reference
A segment to provide a reference relating to the acknowledgement type or the specified error (e.g. functional entity reference such as equipment level).

0210 FTX, Free text
A segment to provide additional details relating to the reference, e.g. the content of the wrong data (and its exact place in the message).

0220 UNT, Message trailer
A service segment ending a message, giving the total number of segments in the message (including the UNH & UNT) and the control reference number of the message.

4.2 Segment index (Alphabetical sequence by tag)

BGM Beginning of message
CNT Control total
COM Communication contact
CTA Contact information
DOC Document/message details
DTM Date/time/period
ERC Application error information
FTX Free text
NAD Name and address
RFF Reference
UNH Message header
UNT Message trailer

4.3 Message structure

4.3.1 Segment table

Pos	Tag	Name	S	R
0010	UNH	Message header	M	1
0020	BGM	Beginning of message	M	1
0030	DTM	Date/time/period	C	9
0040	FTX	Free text	C	9
0050	CNT	Control total	C	9
0060		----- Segment group 1 -----	C	99
0070	DOC	Document/message details	M	1
0080	DTM	Date/time/period	C	99
0090		----- Segment group 2 -----	C	9
0100	RFF	Reference	M	1
0110	DTM	Date/time/period	C	9
0120		----- Segment group 3 -----	C	9
0130	NAD	Name and address	M	1
0140	CTA	Contact information	C	9
0150	COM	Communication contact	C	9
0160		----- Segment group 4 -----	C	99999
0170	ERC	Application error information	M	1
0180	FTX	Free text	C	1
0190		----- Segment group 5 -----	C	9
0200	RFF	Reference	M	1
0210	FTX	Free text	C	9
0220	UNT	Message trailer	M	1

UN Economic Commission for Europe
Palais des Nations, CH-1211 Geneva 10, Switzerland
Tel: +41-22 917 2773 Fax: +41-22 917 0037 E-mail: CEFACT@unece.org

Bijlage 4. Risicoanalyse EDIFORUM

Toelichting op matrix van bedreigingen en maatregelen.

Onderstaande toelichting heeft betrekking op de risicoanalysetabel. Deze tabel is een checklist voor het treffen van maatregelen tegen risico's die EDI met zich meebrengt. In de tabel zelf is aangegeven in hoeverre de bedreiging relevant is voor EDI-I&R (als wellicht zijnde de meest kritische agrarische EDI-toepassing) of andere toepassingen en welke maatregel wordt voorgesteld.

1 Geregistreerde bedreigingen:

1) Frauduleuze zender van berichten.
2) Onbevoegd/onbedoeld aanpassen van het bericht.
3) Onbevoegd/onbedoeld aanpassen van de berichtenstroom.
4) Onbevoegde kennisname berichtinhoud.
5) Onterechte ontkenning van berichtverzending.
6) Onterechte ontkenning van berichtontvangst.
7) Onterecht claimen van berichtontvangst.
8) Verkeerd doorsturen van een bericht.
9) Vertraging in het transport van berichten.
10) Uitvallen van het transport.
11) Onbevoegd kennisname van de berichtenstroom.
12) Onbevoegd maken en verzenden van berichten.
13) Onbevoegde controle en verwerking van berichten.
14) Uitvallen van de EDI-verwerking.
15) Fouten bij bewaren van berichten.

2 Korte omschrijving van de gedefinieerde bedreigingen:

1) Frauduleuze zender van berichten

Hoe kan men er zeker van zijn dat een ontvangen bericht afkomstig is van de genoemde organisatie of persoon? Als de "echtheid" van de zender niet wordt gecontroleerd, bestaat het gevaar dat onbevoegde personen of instanties (concurrenten) opzettelijk de hand leggen op vertrouwelijke informatie betreffende bijvoorbeeld prijzen, produkten of produktieplanningen.

Relevantie

Het is een reeel risico dat derden onbevoegd mutatie-berichten aan I&R zullen aanleveren.

Maatregelen

- gebruik te maken van eigen codes per verzendend systeem; (ID-code/nummer-bron)
- gebruik te maken van eigen codes per verzender; (wachtwoord/pincode)
- op niveau van systeembeheer binnen systemen afschermen applicaties middels passwords;
- uitgebreide logging van verzonden/ontvangen berichten en status van berichten in de vertaalsoftware;
- invoeren van procedures binnen de organisatie die garanderen dat uitsluitend de daartoe geautoriseerde personen berichten mogen aanmaken en versturen;

2) Onbevoegd/onbedoeld aanpassen bericht.

Is het volledige bericht wel ontvangen zoals het werd verzonden? Is het bericht, of een deel ervan, onderweg veranderd? Het is mogelijk een bericht onderweg te onderscheppen en belangrijke informatie te wijzigen voordat het bericht op de plaats van bestemming aankomt.

Is het bericht een duplicaat? Ook met duplicaat berichten kan op een ongewenste manier gemanipuleerd worden.

Relevantie

Er bestaat een reëel risico dat eenzelfde bericht voor een tweede keer of in aangepaste vorm door de verzender wordt aangeleverd. De kans dat de inhoud van een bericht moedwillig veranderd wordt is minimaal. De kans dat de inhoud van het bericht tijdens de transactie per ongeluk veranderd is minimaal.

Maatregelen

- gebruik te maken van codes per verzender;
- uitgebreide logging van verzonden/ontvangen berichten en status van berichten in de vertaalsoftware;
- eventueel kan van een checksum gebruik gemaakt worden.

3) Onbevoegd/onbedoeld aanpassen berichtenstroom.

Bij verstoring van de berichtenstroom kan er verwarring, irritatie en schade ontstaan, bijvoorbeeld door verkeerde of vertraagde inschrijvingen.

Relevantie

Een zekere vertraging van maximaal 2 dagen in het berichtenverkeer leidt niet direct tot grote schade bij partijen.

Maatregelen

- garanties van de netwerkleverancier m.b.t. het uitval-risico van het netwerk;
- vanuit het applicatiebeheer van zowel veehouder als I&R-bureau de vinger aan de pols houden door regelmatige verwerking van ontvangstbevestigingen;
- bij het verzenden van een bericht een volgnummer, datum en tijd meegeven.

4) Onbevoegd kennisname van de berichtinhoud.

Als de inhoud van een bericht geheim moet blijven, hoe wordt er dan voor gezorgd dat het onderweg niet door onbevoegden gelezen wordt?
Dit kan bijvoorbeeld van belang zijn bij het verzenden van bepaalde bedrijfsgegevens (concurrentie overwegingen) en persoonsgegevens (privacy wetgeving).

Relevantie

Weinig relevant voor EDI-I&R. Informatie is niet dermate vertrouwelijk.

Maatregelen

- netwerk biedt voldoende beveiliging dat onbevoegden bericht niet kunnen aftappen.

5) Onterechte ontkenning van berichtverzending.

Het is belangrijk te weten dat de andere partij op een later moment niet kan beweren dat hij niet op de hoogte is van een bericht of de inhoud ervan.

Relevantie

Niet aan de orde. De veehouder heeft geen enkele reden om te ontkennen dat een bericht verstuurd is. Alle partijen hebben er belang bij dat de gegevensuitwisseling snel en soepel verloopt.

Maatregelen

- vanuit de vertaalsoftware wordt automatisch een logging van ontvangen en verstuurde berichten bijgehouden.

6) Onterechte ontkenning van berichtontvangst.

Het is van belang te weten dat de andere partij op een later moment niet kan beweren een bepaald bericht niet ontvangen te hebben. Bijvoorbeeld in het betalingsverkeer kan dit van groot belang zijn om vertragingen bij betalingen te voorkomen.

Relevantie

Zie punt 5.

7) Onterecht claimen van berichtontvangst.

Een valse ontvangst bevestiging bijvoorbeeld kan gebruikt worden om bijvoorbeeld verwarring, irritatie en schade te veroorzaken bij EDI-partijen. Ook kan het gebruikt worden om bepaalde zaken te claimen, bijvoorbeeld orders of bedragen.

Relevantie

Zie punt 5.

8) Verkeerd doorsturen van een bericht (Zoekraken/onjuiste ontvangst)

Het zal duidelijk zijn dat bij zoekraken van een bericht er schade kan ontstaan. Zoekraken kan zowel in het netwerk als in de back office omgeving optreden. Tevens kan bijvoorbeeld door een fout in de applicatie of in de netwerkbehandeling een bericht op een verkeerd adres bezorgd worden.

Relevantie

Reëel risico. Kan gebeuren dat een bericht door foute adressering verkeerd terecht komt.

Maatregelen

- invoeren procedures voor applicatiebeheerder m.b.t. adressenbeheer;

- het maken van backups van alle berichten die worden verstuurd zodat een bericht eventueel voor een tweede keer verstuurd kan worden;
- regelmatig toetsen of een ontvangstbevestiging is ontvangen, is dit niet het geval dan aktie ondernemen.

9) Vertraging in het transport van berichten

- **Ongewenst ontvangen berichten.**
  Indien een systeem wordt overladen met ongewenste berichten komt de verwerking van relevante berichten in gevaar. Ook bij de meervoudige ontvangst van berichten kan er verwarring, irritatie en schade ontstaan, bijvoorbeeld door produktieverlies en/of ten onrechte uitgevoerde leveranties.
- **Vertraagde berichten.**
  De tijd tussen het verzenden en ontvangen van een bericht is met EDI korter dan via de normale postbezorging, waardoor bedrijven in staat zijn "just-in-time" technieken te hanteren. Het is onvermijdelijk dat organisaties afhankelijk worden van deze snelle service. Als berichten echter met vertraging worden bezorgd, kan dit belangrijke negatieve gevolgen hebben.
- **Bericht ten onrechte vaker verzenden.**
  Bij het ten onrechte vaker verzenden van berichten kunnen er bijvoorbeeld ten onrechte uitgevoerde leveranties ontstaan.

Relevantie

Risico is beperkt. Wordt voldoende afgedekt door de basisfunktionaliteit van vertaalsoftware en netwerk.

Maatregelen

- garanties netwerkleverancier;
- uitgebreide logging van berichtenverkeer.

10) Uitval EDI-service

Als een bedrijf eenmaal gebruik maakt van EDI, wordt het ervan afhankelijk. Uitval van de EDI-service (ook tijdelijke) kan al snel tot schade leiden. Er zijn veel oorzaken waardoor de service kan uitvallen, zoals: uitvallen van de computer, storing in de electriciteitsvoorziening, uitvallen netwerksysteem, uitvallen datacommunicatie faciliteiten, defect in de apparatuur van de handelspartner, enz. enz. De matrix volgt de lijn van de brochure, waarin het uitvallen van het transport en het uitvallen van de EDI-verwerking afzonderlijk worden beschreven door het opnemen van beide bedreigingen apart.

Relevantie

Risico is beperkt. De ervaring leert dat de huidige netwerkdiensten meer dan 99 procent operationeel zijn. De informatieoverdracht is daarnaast weinig tijdkritisch. Daarbij komt dat in het geval de applicatie bij zender of ontvanger uitvalt de postbus als buffer fungeert. In extreme situatie kan uitgeweken worden naar Voice-respons.

Maatregelen

- garanties netwerkleverancier;
- invoeren procedures van wat te doen in het geval het netwerk uitvalt of de applicatie bij zender/ontvanger uitvalt.

11) Onbevoegde kennisname berichtenstroom.

Als de berichtenstroom in een netwerk gevolgd kan worden, komt allerlei informatie vrij over relaties tussen partijen in het netwerk. Zo is het voor een leverancier zeer interessant om er achter te komen wie zijn concurrenten zijn door te volgen bij wie (mogelijke) klanten hun bestellingen plaatsen.

Relevantie

Risico is beperkt. Informatie is weinig vertrouwelijk.

Maatregelen

- wordt voldoende afgedekt door huidige funktionaliteit netwerk.

12) Onbevoegd maken/verzenden van berichten.

De bedreigingen bij het genereren van uitgaande berichten liggen voornamelijk op het gebied van de invoer van gegevens, de goede werking van de applicatie en de toegangsbeveiliging tot de gegevens en de applicatie.

Relevantie

Risico is reëel. Moet vooral afgedekt worden aan de kant van de applicatie en systeembeheerder.

Maatregelen

- invoeren procedures m.b.t. de autorisatie van personen die berichten mogen aanmaken.

13) Onbevoegde verwerking en controle van binnenkomende berichten.

De bedreigingen bij het verwerken van binnenkomende berichten liggen eveneens voornamelijk op het gebied van de invoer van gegevens (invoercontroles), de goede werking van de applicatie en de toegangsbeveiliging tot de gegevens en de applicatie.

Relevantie

Risico is reëel. Moet vooral afgedekt worden aan de kant van de applicatie en syteembeheerder.

Maatregelen

- invoeren procedures m.b.t. de autorisatie van personen die berichten mogen verwerken.

14) Uitvallen van de EDI-verwerking

Zie 10

15) Fouten bij bewaren van berichten.

Er zijn diverse redenen om de gegevens afkomstig uit het EDI-verkeer te bewaren, zoals:
het nakomen van wettelijke eisen en voorschriften, het leveren van bewijs van transacties, het leveren van informatiebronnen voor planning- en marketing strategieën, enz., enz.
De mate waarin bewaarde gegevens worden beveiligd hangt af van het gebruik dat men er van wil maken.
De bewaarde gegevens moeten worden beschermd tegen wijziging, vernietiging en openbaarmaking.

Relevantie

Risico is reëel. Moet vooral afgedekt worden aan de kant van de applicatie en syteembeheerder.

Maatregelen

- invoeren procedures m.b.t. de autorisatie van personen die berichten mogen aanmaken.

Toelichting bij de kolommen van de matrix

nr. Geeft het referentie nummer aan van een bedreiging.

bedreiging Omschrijving van de bedreiging.

kwaliteitseis Deze kolom geeft de drie kwaliteits-eisen aan, welke een rol spelen bij het beveiligen van het EDI-verkeer. Een bedreiging zou het berichten verkeer op één of meer van de aangegeven kwaliteiten kunnen aantasten.
De drie kwaliteits-eisen zijn respectievelijk:

- **Betrouwbaarheid,** afgekort: **BT**
- **Vertrouwelijkheid,** afgekort: **VT**
- **Beschikbaarheid,** afgekort: **BS**

niveau In deze kolom worden de gebieden aangegeven waarop de maatregelen genomen kunnen worden, te weten:

- **Inhoud+Transactie** afgekort: **I**
  ("berichten"-niveau)
- **Back Office**
  (de kantoor en/of automatiserings-organisatie)
  onderverdeeld in:
  - **Systeembeheer,** afgekort: **SB**
  - **Applicatiebeheer,** afgekort: **AB**
  - **Gegevensbeheer,** afgekort: **GB**
  - **Netwerkbeheer(intern),** afgekort: **NB**
  - **Netwerk** afgekort: **N**
    (de voorzieningen die (meestal) door een derde partij geleverd worden om het bericht electronisch te transporteren van zender naar ontvanger),

maatregel Omschrijving van gewenste maatregelen tegen de gerelateerde bedreigingen.

beveiligings-klasse Beveiligings-classificatie van de aangegeven maatregel in
Essentieel en Speciaal, waarbij:

- **Essentieel** aangeeft dat het hier een maatregel betreft die nodig geacht wordt voor het realiseren van een, algemeen aanvaard, minimum niveau van beveiliging (de "Baseline").
- **Speciaal** aangeeft dat het hier een maatregel betreft die extra beveiliging kan bieden in bepaalde, bijzondere, situaties. Implementatie geschiedt in het algemeen pas na een grondige afweging van de risico's.

Per toepassing moet worden aangegeven welke aspecten relevant zijn. De tabel is voorlopig alleen voor EDI-I&R ingevuld.

In de tabel is aangegeven in hoeverre het relevant is voor de EDI-I&R-toepassing en wat de eventuele maatregelen moeten zijn.

Nr.	Bedreiging	Kwaliteitseis			Niveau	Maatregel	Beveiligingsklasse							
		BT	VT	BS			essen-tieel	spec iaal	EDI-I&R	EDI-dhz-KI	EDI-EMM	EDI-NRS	EDI-dap	EDI-zuivel
1	Frauduleuze zender	x			I	Authenticiteitswaarborging d.m.v. encryptie en/of checksum (digitale handtekening)		x						
		x			I	Authenticiteitswaarborging d.m.v. encryptie en/of checksum (digitale handtekening + 2e man controle)		x						
		x			SB	Authenticiteits-controle op basis van : ID-code + Pas		x						
		x			SB	Authenticiteits-controle op basis van : ID-code + Wachtwoord	x		x					
		x			SB	Authenticiteits-controle op basis van : ID-code + Wachtwoord + Pas		x						
		x			SB	Authenticiteits-controle op basis van : ID-code + Chipcart		x						
		x			SB	Checkpointing (geprogrammeerde controles en transactieprofielen)		x						
		x			N	Fysieke toegangsbeveiliging kritische netwerkfaciliteiten (b.v. modems en routers)		x						
		x			N	Logische toegangsbeveiliging netwerkfaciliteiten (b.v. routercontrole)		x						
2	Onbevoegd/onbedoeld aanpassen van het bericht	x			I/N	Foutdetectie (correctiecode (checksum))	x		x					
		x			AB	Ontvangstbevestiging	x		x					
		x			AB	Berichtvolgordenummering		x						
		x			AB	Bewaring en herziening	x		x					
		x			I	Checksum en encryptie		x						
		x			SB	Checkpointing (geprogrammeerde controles en transactieprofielen)		x						
		x			N	Fysieke toegangsbeveiliging netwerkfaciliteiten	x		x					
3	Onbevoegd/onbedoeld aanpassen berich-tenstroom	x			AB	Berichtvolgordenummering + Datum- en Tijdsaanduiding	x		x					

Nr.	Bedreiging	Kwaliteitseis			Niveau	Maatregel	Beveiligingsklasse							
		BT	VT	BS			essen-tieel	spec iaal	EDI-I&R	EDI-dhz-KI	EDI-EMM	EDI-NRS	EDI-dap	EDI-zuivel
		x			AB	Ontvangstbevestiging	x		x					
				x	SB	Bewaring mutatie-files i.v.m. herstelacties		x						
		x			N	First-In First-Out garantie Netwerk-leveranciers		x						
4	Onbevoegd kennisname berichtinhoud		x		I	Encryptie	x							
			x		SB	Sleutelbeheer en gegevens- en documentenbeheer	x							
			x		N	Toegangsbeveiliging netwerkfaciliteiten (fysiek en logisch)	x							
5	Onterechte ontkenning van berichtverzen-ding	x			GB	Registratie van ontvangen berichten	x		x					
		x			I	Authenticiteitsvaststellling van verzender d.m.v. encryptie (digitale handtekening)		x						
		x			I	Electronische notarisfunktie		x						
		x			AB	Logging van ontvangstbevestiging	x		x					
		x			N	Aktiviteitenregistratie netwerk		x						
6	Onterechte ontkenning van berichtont-vangst	x			GB	Registratie van ontvangen berichten	x		x					
		x			I	Authenticiteitsvaststellling van verzender d.m.v. encryptie (digitale handtekening)		x						
		x			I	Electronische notarisfunktie		x						
		x			AB	Logging van ontvangstbevestiging	x		x					
		x			N	Aktiviteitenregistratie netwerk		x						
7	Onterecht claimen van berichtontvangst	x			I	Encryptie		x						
		x			SB	Authenticiteitscontrole (zie ook nr. 1)	x							
		x			AB	Logging van ontvangstbevestiging (bij ontvanger)	x		x					
		x			NB	Fysieke- en logische toegangsbeveiliging	x		x					

Nr.	Bedreiging	Kwaliteitseis			Niveau	Maatregel	Beveiligingsklasse							
		BT	VT	BS			essen-tieel	spec iaal	EDI-I&R	EDI-dhz-KI	EDI-EMM	EDI-NRS	EDI-dap	EDI-zuivel
		x			N	Toegangsbeveiliging intern netwerk + Aktiviteitenregistratie netwerk	x		x					
8	Verkeerd doorsturen van bericht (zoek raken/onjuiste ontvangst)	x			AB	Adresserings-controle + Retournering bericht	x		x					
				x	AB/GB	Registratie van berichten (vastleggen/bewaren)	x		x					
				x	AB	Herverzending na uitblijven ontvangstbevestiging	x		x					
				x	NB	Alarmering na verlopen ontvangtsbevestigingsperiode		x						
				x	N	Aflevergarantie Netwerk leverancier + Aktiviteitenregistratie Netwerk		x						
9	Vertraging in transport van berichten													
	ongewenst ontvangen berichten			x	NB	Beperking beschikbaarheid netwerkadressen		x						
			x	x	AB	Melding aan verzender	x		x					
			x	x	N	Aflevergarantie Netwerk Leverancier	x		x					
	vertraagde berichten			x	NB	Optimalisering intern netwerksysteem		x						
				x	N	Capaciteitsgarantie Netwerkleverancier + Rouleren	x		x					
	bericht ten onrechte vaker verzenden			x	I	Bericht identificatie (b.v. electr. handtekening, nummering, datum- en tijdsaanduyiding)	x		x					
				x	AB	Ontvangstbevestiging		x	x					
10	Uitvallen van het transport			x	SB	Een calamiteitenplan opstellen en regelmatig testen	x		x					
				x	SB	Berichten bewaren en reserve kopieën maken	x		x					
				x	GB	Backup voorzieningen (inc. externe opslag backup-bestanden)	x		x					
				x	N	Netwerk uitwijkplan, waarin meervoudige verbindingen		x						
11	Onbevoegde kennisname berichtenstroom		x		AB	Continue verzending (inbedding relevante informatie in niet relevante informatie)		x						

Nr.	Bedreiging	Kwaliteitseis			Niveau	Maatregel	Beveiligingsklasse							
		BT	VT	BS			essen-tieel	spec iaal	EDI-I&R	EDI-dhz-KI	EDI-EMM	EDI-NRS	EDI-dap	EDI-zuivel
			x		N	Dynamische netwerkverbindingen		x						
			x		N	Versluiering netwerkadressen		x						
			x		N	Fysieke en logische netwerkbeveiliging	x		x					
12	Onbevoegd maken/verzenden van berich-ten	x			AB	Invoer-validaties + foutmeldingen	x		x					
13	Onbevoegde controle/verwerking van be-richten	x			AB	Opslag binnenkomende berichten en foutmeldingen	x		x					
		x			AB	Invoer-validaties + foutmeldingen	x		x					
14	Uitvallen van de EDI-verwerking			x	SB	Een calamiteitenplan opstellen en regelmatig testen	x		x					
				x	SB	Berichten bewaren en reserve kopieën maken	x		x					
				x	GB	Backup voorzieningen (incl. externe opslag backup-bestanden)	x		x					
15	Fouten bij het bewaren van berichten			x	GB	Checksum genereren en bewaren	x		x					
				x	GB	Berichten bewaren en reserve kopieën maken (incl. checksum)	x		x					

Nr	DEEL B Bedreiging	Tabel kosten/baten per maatregel. maatregel	EDI-I&R	Schatting	
				Kosten	Baten
1	Frauduleuze zender	Authenticiteits-controle op basis van : ID-code + Wachtwoord	**X**		
2	Onbevoegd/onbedoeld aanpassen van het bericht	Foutdetectie (correctiecode (checksum))	X		
		Ontvangstbevestiging	X		
		Bewaring en herziening	X		
		Fysieke toegangsbeveiliging netwerkfaciliteiten	X		
3	Onbevoegd/onbedoeld aanpassen berichtenstroom	Berichtvolgordenummering + Datum- en Tijdsaanduiding	X		
		Ontvangstbevestiging	X		
5	Onterechte ontkenning van berichtverzending	Registratie van ontvangen berichten	X		
		Logging van ontvangstbevestiging	X		
6	Onterechte ontkenning van berichtontvangst	Registratie van ontvangen berichten	X		
		Logging van ontvangstbevestiging	X		
7	Onterecht claimen van berichtontvangst	Logging van ontvangstbevestiging (bij ontvanger)	X		
		Fysieke- en logische toegangsbeveiliging	X		
		Toegangsbeveiliging intern netwerk + aktiviteitenregistratie netwerk	X		
8	Verkeerd doorsturen van bericht (zoek raken/onjuiste ontvangst)	Adresserings-controle + Retournering bericht	X		
		Registratie van berichten (vastleggen/bewaren)	X		
		Herverzending na uitblijven ontvangstbevestiging	X		
9	Ongewenst ontvangen berichten	Melding aan verzender	X		
		Aflevergarantie Netwerk Leverancier	X		
	Vertraagde berichten	Capaciteitsgarantie Netwerkleverancier + Rouleren	X		
	Bericht ten onrechte vaker verzenden	Bericht identificatie (b.v. electr. handtekening, nummering, datum- en tijdsaanduiding)	X		
		Ontvangstbevestiging	X		
10	Uitvallen van het transport	Een calamiteitenplan opstellen en regelmatig testen	X		
		Berichten bewaren en reserve kopieën maken	X		
		Backup voorzieningen (inc. externe opslag backup-bestanden)	X		
11	Onbevoegde kennisname berichtenstroom	Fysieke en logische netwerkbeveiliging	X		
12	Onbevoegd maken/verzenden van berichten	Invoer-validaties + foutmeldingen	X		
13	Onbevoegde controle/verwerking van berichten	Opslag binnenkomende berichten en foutmeldingen	X		
		Invoer-validaties + foutmeldingen	X		
14	Uitvallen van de EDI-verwerking	Een calamiteitenplan opstellen en regelmatig testen	X		
		Berichten bewaren en reserve kopieën maken	X		
		Backup voorzieningen (incl. externe opslag backup-bestanden)	X		
15	Fouten bij het bewaren van berichten	Checksum genereren en bewaren	X		
		Berichten bewaren en reserve kopieën maken (incl. checksum)	X		

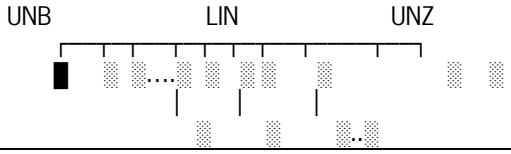
Bijlage 5. EDIFACT syntax

Edifact kent een hiërachische opbouw in segmenten.

Een berichtuitwisseling tussen een zender en ontvanger wordt een interchange genoemd. Deze wordt aangeduid met kopsegment UNB en staartsegment UNZ. Binnen een interchange kunnen meerdere berichten worden uitgewisseld, berichten worden met respectievelijk kop staart aangeduid met het UNH- en UNT-segment.

Er zijn dus twee headers (en trailers).
Onderstaand de inhoud ervan zoals bij EDI-veevoer wordt toegepast.

Interchangeheader:

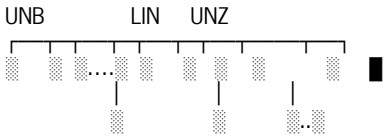


UNB	INTERCHANGE HEADER	M		
S001	SYNTAX INDENTIFIER	M		
0001	Syntax indentifier	M	a4	*'UNOA'*
0002	Syntax version number	M		*'2'*
S002	INTERCHANGE SENDER	M		
0004	Sender identification	M	an..35	*Verzenders-nummer*
0007	Identification code qualifier	C	an..4	-
0008	Address for reverse routing	C	an..14	-
S003	INTERCHANGE RECIPIENT	M		
0010	Recipient indentification	M	an..35	*Ontvangers-nummer*
0007	Identification code qualifier	C	an.4	-
0014	Routing address	C	an.14	-
S004	DATE/TIME OF PREPARATION	M		
0017	Date	M	n6	*Verzenddatum (YYMMDD)*
0019	Time	M	n4	*Verzendtijd (UUMM)*
0020	INTERCHANGE CONTROL REFERENCE	M	an..14	*Interchangevolgnummer*
S005	RECIPIENTS REFERENCE, PASSWORD	C		
0022	Recipient's reference/password	M	an..14	-
0025	Recipients's refer./passw. qualifier	C	an2	-
0026	APPLICATION REFERENCE	C	an..14	-
0029	PROCESSING PRIORITY CODE	C	a1	-
0031	ACKNOWLEDGEMENT REQUEST	C	n1	-
0032	COMMUNICATION AGREEMENT	C	an..35	-
0035	TEST INDICATOR	C	n1	-

Verplicht segment. Wordt éénmaal opgenomen. Dit segment geeft de identificatie en de start aan van een interchange.

Verplicht:
0001 = 'UNOA', hetgeen betekent dat gebruik wordt gemaakt van karakterset A
0002 = '2'
0004 = Het postbusnummer van de verzender
0010 = Het postbusnummer van de ontvanger
0017 = Datum van aanmaak van de interchange in formaat YYMMDD
0019 = Tijd van aanmaak van de interchange in formaat UUMM (00<UU<24)
0020 = Een door de verzender te genereren uniek nummer om de interchange te identificeren t.b.v. verzoeken om nogmaals de interchange op te starten bij storingen, fouten e.d..

Interchangestaart:



UNZ,	INTERCHANGE TRAILER, M, 1 x			
0036	INTERCHANGE CONTROL COUNT	M	n..6	*Aantal berichten in de interchange*
0020	INTERCHANGE CONTROL REFERENCE	M	an..14	*Referentienummer*

Verplicht segment, dat één keer voorkomt. Geeft het einde van de interchange aan.

Verplicht:
0036 = Aantal berichten in de interchange
0020 = Referentienummer dat gelijk is aan het data-element 0020 in het UNB segment.

Berichtheader:

UNH,	MESSAGE HEADER, M, 1 x			
0062	MESSAGE REFERENCE NUMBER	C	an..14	
S009	MESSAGE IDENTIFIER	C		
0065	Message type identifier	C	an..6	'INVOIC'
0052	Message type version number	C	an..3	'D'
0054	Message type release number	C	an..3	'93A'
0051	Controlling agency	C	an..2	'UN'
0057	Association assigned code	C	an..6	'EVF1.0'
0068	COMMON ACCESS REFERENCE	C	an..35	
S010	STATUS OF TRANSFER	C		
0070	Sequence message transfer number	C	n..2	
0073	First/last message transfer ind.	C	a1	

Verplicht segment waarin de bijzonderheden over het bericht staan vermeld; dit segment komt één keer voor

0062 = Uniek berichtnummer, te bepalen door verzender.
0057 = 'EVF1.0' (EDI-veevoer factuurbericht versie 1.0)

Berichtstaart:

UNT,	MESSAGE TRAILER M, 1 x			
0074	MESSAGE OF SEGMENTS IN A MESSAGE	C	n..6	
S009	MESSAGE REFERENCE NUMBER	C	AN..14	

Bijlage 6. EbXML: uitwerking voor agrarische EDI-toepassingen

Een voorbeeld op basis van EDI-NRS.

```
From: edi@nrs.nl
To: jansen@example.com
Date: Thu, 08 Feb 2001 19:32:11 CST
MIME-Version: 1.0
SOAPAction: "ebXML"
Content-type: multipart/related; boundary="BoundarY"; type="text/xml";
          start="<ebxhmheaderlll@nrs.nl>"

--BoundarY
Content-ID: <ebxhmheaderlll@nrs.nl>
Content-Type: text/xml

<SOAP-ENV:Envelope xmlns:SOAP-ENV='http://schemas.xmlsoap.org/soap/envelope/'
   xmlns:eb='http://www.ebxml.org/namespaces/messageHeader'>
<SOAP-ENV:Header>
   <eb:MessageHeader SOAP-ENV:mustUnderstand="1" eb:version="1.0">
      <eb:From>
         <eb:PartyId type="REL">10000213</eb:PartyId>
      </eb:From>
      <eb:To>
         <eb:PartyId type="UBN">102445</eb:PartyId>
      </eb:To>
      <eb:CPAId>1</eb:CPAId>
      <eb:ConversationId>1</eb:ConversationId>
      <eb:Service type="APPLICAT">2100</eb:Service>
      <eb:Action>1</eb:Action>
      <eb:MessageData>
         <eb:MessageId>nrs.nl.1</eb:MessageId>
         <eb:Timestamp>2001-02-15T11:12:12Z</Timestamp>
      </eb:MessageData>
   </eb:MessageHeader>
</SOAP-ENV:Header>
<SOAP-ENV:Body>
   <eb:Manifest eb:id="Manifest" SOAP-ENV:mustUnderstand="1" eb:version="1.0">
      <eb:Reference xlink:href="cid:ebxmlpayloadlll@nrs.nl">
         <eb:Schema location="http://www.atc.nl/schemas/501v44.mpd" version="4.4"/>
      </eb:Reference>
   </eb:Manifest>
</SOAP-ENV:Body>
</SOAP-ENV:Envelope>

--BoundarY
Content-ID: <ebxmlpayloadlll@nrs.nl>
Content-type: application/zip
Content-Disposition: attachment; filename="EdiNrs.zip"
Content-transfer-encoding: base64

UEsDBBQAAAAIAONtpCqKVL7whAQAADARAAAWAAAAVEVTVDA3LTMxMC0xMTAgdHZkLmVkac1YyXKz
OBC+T9W8Azf/UypcklilmwCxJCD4BWSSvP+DTIvFxgI7TmqmapJD4t6/Vm/JqBI0qlZwiuKI+NQj
…
xMfYw5z4V0IAJEPAGPs45MSjIep1On/EBEcIeQSf/vxjVKXF+D22g+x5xhkTfFQ8yzE4ANGkaIwS

--BoundarY--
```

Figuur 19 Voorbeeld ebXML envelop voor EDI-NRS (via SMTP)

Toelichting op de elementen in <eb:MessageHeader>:

1. Identificatie van de zender en de ontvanger:
   ```
   <eb:From><eb:PartyId type="REL">10000213</eb:PartyId></eb:From>
   <eb:To><eb:PartyId type="UBN">102445</eb:PartyId></eb:To>
   ```
2. Het CPA Id in ebXML is verplicht en verwijst naar de gemaakte uitwisselings afspraken tussen de zender en de ontvanger. Omdat in de agrarische wereld momenteel dergelijke CPA's niet worden gebruikt is hier een fictieve waarde ingevuld:
   ```
   <eb:CPAId>1</eb:CPAId>
   ```
3. Het (verplichte) element ConversationId maakt het mogelijk om verschillende berichten die bij elkaar horen (die bijv. één transactie vormen zoals een order en order-respons) één unieke id te geven. In het voorbeeld (EDI-NRS) bericht heeft dit geen functie en is hier een fictieve waarde ingevuld:
   ```
   <eb:ConversationId>1</eb:ConversationId>
   ```
4. De verplichte elementen Service en Action zorgen ervoor dat het bericht bij de ontvanger aan het juiste proces wordt aangeboden. Het is dus enigszins vergelijkbaar met het Agrotel gegeven 'FileType' en het Adis-headerelement 'Applicatie ontvanger', vandaar dat hier dit laatste gegeven is ingevuld. Het type 'APPLICAT' verwijst naar de betreffende ADED coderingenlijst. Bij Action is een fictieve waarde ingevuld:
   ```
   <eb:Service type="APPLICAT">2100</eb:Service>
   <eb:Action>1</eb:Action>
   ```
5. MessageId is een unieke identificatie van dit ebXML bericht. In een evt. fout- of bevestigings-bericht wordt hiernaar verwezen. In Timestamp staat de aanmaakdatum van dit ebXML bericht:
   ```
   <eb:MessageData>
     <eb:MessageId>nrs.nl.1</eb:MessageId>
     <eb:Timestamp>2001-02-15T11:12:12Z</Timestamp>
   </eb:MessageData>
   ```

Toelichting op de elementen in <eb:Manifest>:

6. Het element Reference verwijst naar de te verzenden data (de payload bijv. een Adis- of XML-bericht). In dit geval wordt verwezen naar de content-id van de attachment met het (gezipte) EDI-NRS bericht. In ebXML kan men meerdere Reference elementen opgeven:
   ```
   <eb:Reference xlink:href="cid:ebxmlpayloadlll@nrs.nl">
   ```
7. M.b.v het (optionele) element Schema kan verwezen worden naar een bepaalde berichtdefinitie. Dit kan een XML Schema of DTD zijn maar ook een ander soort definitie. Deze elementen kan men dus vergelijken met de Adis-headerelementen 'Berichttype' en 'Versienr berichttype', met dit verschil dat er hier naar een fysiek document wordt verwezen:
   ```
   <eb:Schema location="http://www.atc.nl/schemas/501v44.mpd" version="4.4"/>
   ```

Mits het laatst genoemde element (Schema) wordt opgenomen bevat deze envelop de belangrijkste informatie om een willekeurig bericht te kunnen verwerken: wat is het en waar komt het vandaan. Als men niet wil verwijzen naar een bepaald berichtdefinitie-document maar alleen een berichttype-id (zoals nu in de Adis-header 800010) dan kan men er ook voor kiezen om een eigen element toe te voegen. Dit is binnen ebXML mogelijk, bijv.:

```
<eav:MessageType type="501" version="4.4"/>
```

De namespace ('eav') moet dan wel aan het begin gedefinieerd worden, bijv.:

```
xmlns:eav='http://www.atc.nl/namespaces/eavMessageHeader'
```

Mapping huidige headers op ebXML

DD-nr	Naam header gegevenselement	Mapping naar ebXML	V/O/C	Cat
000000	Aanduiding datadictionary	Kan vervallen, vermelden berichttype + versienr is voldoende.		A
201685	Datadictionary-versie	Idem		A
800001	Berichttype	Komt functioneel overeen met: <eb:Schema location="…" version="…"/>	O	A
800002	Versienummer berichttype	Is attribuut 'version' in element 'Schema'	O	A
800009	Releasenummer berichttype	Kan vervallen, vermelden berichttype + versienr is voldoende.		A
800006	beheerder berichttype	Idem		A
800007	Berichtspecificatie	Idem		A
150000	soort-zender	Kan vervallen (mits zender en ontvanger elkaar kennen)		A
150001	soort-ontvanger	Kan vervallen (mits zender en ontvanger elkaar kennen)		A
150002	soort-bericht	Kan vervallen, vermelden berichttype + versienr is voldoende.		A
800004	bericht id	<eb:MessageData> <eb:MessageId> … Mits er maar 1 att. is per envelop!	V	E
201575	Bestandsdatum	<eb:MessageData> <eb:Timestamp> …	O	E
201576	Bestandstijd	Zie Timestamp		E
205003	zender id.	<eb:from> <eb:PartyId> …	V	E
204220	Type zender-id	<eb:from> <eb:PartyId type="…">	C	E
205004	ontvanger id.	<eb:to> <eb:PartyId> …	V	E
204221	Type ontvanger-id	<eb:to> <eb:PartyId type="…">	C	E
205006	applicatie ontvanger	<eb:Service type="APPLICAT">….</eb:Service>	V	E
203984	Ind-ontvangst-bevestiging	<eb:QualityOfServiceInfo eb:deliveryReceiptRequested="…">	O	E
860090	Referentie berichtId	<eb:MessageData> <eb:RefToMessageId> …	C	E
B0001	Syntax identifier (character set)	Content-Type: text/xml; charset="…" of <?xml version="1.0" encoding="…" ?> Indien beide opgenomen dan moeten ze gelijk zijn.	O ?	E
B0002	Syntax version number	Een characterset in ebXML heeft geen versienr.		E
B0020	Interchange control reference	<eb:MessageData> <eb:MessageId> …	V	E
B0026	Application reference	Zie applicatie ontvanger		E
B0032	Communication agreement	<eb:CPAId> …	V	E
B0025	Recipient's ref./passw.qualifier	Zie Wachtwoord.		Ea
202852	Legaliteitscode	Zie Wachtwoord.		Eb
800008	Eventteller	Kan nu gebruikt worden om te controleren of alle data-regels zijn ontvangen. Als in de ebXML-envelop deliverySemantics="OnceAndOnlyOnce" is opgegeven dan moet de MSH reliableMessagingMethod ondersteunen (of anders een foutcode teruggeven). Zie ook volgende paragraaf.		Eb
203881	Pincode	Zie Wachtwoord.		Eb
860077	Wachtwoord	In een ebXML-envelop kan een digitale handtekening worden opgenomen. Zie volgende paragraaf.		Eb
860075	Retour-medium	Zie Retour-adres.		En
860076	Retour-adres	In ebXML legt men in het autorisatiecontract (CPP/CPA) vast hoe de berichtenstroom moet lopen. Eventueel kan men in de MIME-envelop een 'Reply-To:' opnemen maar een MSH mag dit negeren.		En

Figuur 20 Mapping ebXML elementen op huidige ADIS elementen

Ten behoeven van de mapping naar ebXML zijn de header gegevenselementen ingedeeld naar de volgende categorieën:

A Autorisatiegegeven: vaste instellingen voor een bepaalde gegevensuitwisseling die men onderling of in het betreffende EDI-project zijn overeengekomen, zoals berichttype en te gebruiken datadictionary. Hoort thuis in de bericht-header/envelop of (zoals in ebXML) in een uitwisselingsovereenkomst.

E Bericht gegeven dat ook standaard voorkomt in ebXML.

Eb Bericht gegeven met een beveiligingsaspect dat door ebXML wordt afgedekt.

En Bericht gegeven uit de netwerk-envelop (MIME) van ebXML.

B Bericht gegeven: algemeen bericht gegeven, is berichttype onafhankelijk en hoort dus thuis in de bericht-header maar is niet standaard opgenomen in ebXML.

BS Berichttype specifiek gegeven: hoort dus niet in een algemene bericht-header/envelop.

X Bericht gegevens die in principe niet meer nodig of dubbel zijn.

In bovenstaand overzicht zijn alleen de header gegevenselementen uit categorie A en E opgenomen omdat die evt. vervangen kunnen worden door ebXML-envelop elementen. De overige elementen moeten in de bericht-header blijven (of kunnen zelfs geheel vervallen).

Bijlage 7. FTP toepassingen in de agrarische sector

In deze bijlage een detailbeschrijving van de FTP-toepassingen in de agrarische sector.

Bijlage 7.1. NRS

Uitwisseling data door gebruiker/veehouder
Bij de start is een bewuste keuze gemaakt om zich niet te bemoeien met het aanleveren van de data. Het aantal potentiële klanten (+/- 10.000 boeren) en de bezinning op haar kerntaken is voor het NRS reden geweest om dit over te laten aan softwareleveranciers. In de praktijk zien we nu EDI-communicatie volgens de volgende kanalen:

- Gestuurd (automatisch) vanuit een aantal MIS-en
- Semi-automatische of handmatige ftp-sessies mbv gewone ftp-cliënts, aangestuurd door veehouder zelf. De veehouder maakt connectie en geeft opdrachten tot verzenden c.q. ophalen bestanden, verwijderen e.d. (bestandsbeheer).
- Nieuwe applicaties, waaronder mogelijk ook op zich staande web-applicaties

Alhoewel het NRS het liefst geleid transport vanuit het MIS ziet heeft men dit dus niet in de hand. Dit wordt mede veroorzaakt doordat men niet heeft gekozen voor een volledig servergestuurd proces. De keuze om het aanleveren (ophalen) van data over te laten aan derden heeft consequenties:

1. Geen – of niet altijd - sturing van het proces. De kans op (menselijke) fouten is reëel
2. Invulling retourberichten moeilijker. Het opzetten en verwerken van retourberichten is een proces waarbij men deels afhankelijk is van de cliënt.

Beveiligingsaspecten
Er is uiteraard aandacht besteed aan de beveiligingsaspecten. Autorisatie vindt plaats door een webster-applicatie.
(Nog) geen of onvoldoende aandacht is er voor:

- **Encryptie/versleuteling van data**
  Theoretisch vraagt transport over internet om aandacht hiervoor, Zeker als (naar de nabije toekomst toe) bedrijfskritische en mogelijk juridisch gevoelige data over het internet wordt gestuurd.
- **Authenticatie**
  Wel op het laagste niveau van autorisatie, maar niet via technieken als (public/private) keys e.d.. Alhoewel alle gebruikers eigen autorisatiecodes hebben lijkt het goed mogelijk om zich voor te doen als een andere gebruiker.
- **Logging**
  Op dit moment wordt nog onvoldoende of te weinig inzichtelijke logging van sessies op klant- en systeemniveau gedaan. Met name vanuit intern beheersmatig aspect is het nu moeilijk om goed overzicht te houden, naarmate het aantal deelnemende veehouders mee gaat doen wordt dit probleem groter.

Genoemde beveiligingsaspecten (m.n. encryptie en authenticatie) worden op dit door het NRS nog niet gezien als hot-items.

Bestandsbeheer
Het ftp-gebied van de gebruiker op de server lijkt, zeker bij het gebruik van meerdere EDI-toepassingen, nogal complex van aard. Het proces van over- en klaarzetten van databestanden is omgeven door een ietwat omslachtige procedure, waarbij gevraagd wordt om enige bestandbeheeracties als zenden, hernoemen en verwijderen.
Indien dit proces automatisch wordt aangestuurd is er niet echt een probleem. Als er 'handmatig' met ftp acties moeten worden ondernomen dan is de kans op fouten of vergissingen niet onmogelijk. Een en ander lijkt overigens vooralsnog niet snel te kunnen leiden tot echt fatale fouten, eerder wel extra werk door de beheerder.

Aandachtsgebieden / knelpunten
De volgende gebieden vragen om aandacht:

1. Sturing van het proces van aanleveren data, hoe invloed hierop te krijgen ?

- Nagedacht zou moeten worden hoe de communicatie van losse ftp-cliënts zoveel mogelijk teruggedrongen kan worden. Wellicht is toch het voorschrijven (evt. aanschaffen of ontwikkelen) van een volledig gestuurde ftp-schil een oplossing.
- Overwogen kan worden om gebruik te maken van servergestuurde communicatieprocessen waarbij bijvoorbeeld gebruik wordt gemaakt van een script welk steeds per sessie wordt gegenereerd op de server, wordt opgehaald door de cliënt en wordt uitgevoerd vanaf de cliënt.

2. Invulling retourberichten
3. Omslachtige bestandsbeheer als onderdeel van de communicatiesessie
   Door meer automatische sturing van dit proces aan te moedigen zal dit minder een probleem worden
4. Aanscherping beveiligingsaspecten i.r.t. aanscherping eisen , bijvoorbeeld door I&R

Bijlage 7.2. Zuivelnet

Beheersorganisatie en structuur
De ftp-omgeving van Zuivelnet is opgezet door AgiS automatisering. Omdat deze automatiseerder ook betrokken is geweest bij de opzet van de FTP-NRS omgeving lijken deze omgevingen in veel opzichten op elkaar.

Een opvallend verschil tussen de twee omgevingen is hier het ontbreken van de complexiteit van de gebruikersomgeving op de server. Melkveehouders **halen enkel gegevens op** van de Zuivelnet-ftp server, daarnaast is het aantal berichten dat via hetzelfde kanaal (op dit moment) uitgewisseld wordt geringer, dit ondanks dat ook meteogegevens en updates via deze ftp-server opgehaald kunnen worden. Door de grotere eenvoud van Zuivelnet is de bestandsstructuur op de server, en daarmee de (handmatige) bestandsbeheershandelingen (als hernoemen, verwijderen bestanden), minder complex .

Bij de opzet is een duidelijke keuze gemaakt voor uitwisseling middels ftp en niet per e-mail, dit om de reden dat naar mening van de ontwikkelaar enkel met ftp een gecontroleerde dataoverdracht te bewerkstelligen is. Gebruik van e-mail betekent dat de controle over het transport uit handen gegeven wordt, het is dan niet bekend waar het bericht is, hoelang deze onderweg zal zijn en of deze überhaupt wel aankomt op de plaats van bestemming.

Uitwisseling data door gebruiker/veehouder
Voor het aanleveren van data is bij Zuivelnet in grote lijnen voor dezelfde strategie gekozen als bij NRS: de gebruiker bepaald in principe zelf welke (standaard) ftp-cliënt hij/zij gebruikt.
Ook hier zien we dan in de praktijk de volgende mogelijkheden:

- Gestuurd (automatisch) ftp-sessies vanuit een aantal MIS-en.
- Semi-automatische of handmatige ftp-sessies mbv gewone ftp-cliënts, aangestuurd door veehouder zelf. De veehouder maakt connectie en geeft opdrachten tot verzenden c.q. ophalen bestanden, verwijderen e.d. (bestandsbeheer).
- En naar de toekomst de mogelijkheid van nieuwe applicaties, waaronder mogelijk ook op zich staande web-applicaties

Vanwege de bezwaren van het ongestuurd gebruik van zo maar een ftp-cliënt biedt Zuivelnet de mogelijkheid om een aangepaste windows ftp-cliënt (qftp/quick ftp) te downloaden en te gebruiken. De volgende relevante functionaliteit is in dit pakket ingebouwd, welke niet standaard altijd in andere ftp-cliënts aanwezig is:

- Handmatig ophalen (evt. versturen) bestanden met ingestelde in- en out directory's.
- Multi-ftp sessies: ophalen of versturen bestanden van/naar meerdere ftp-servers.
- Commandline aansturing, waardoor geautomatiseerde ftp-sessies via bijvoorbeeld de taakplanner of programma's van derden mogelijk worden.
- Controle op daadwerkelijke en foutloze overdracht van de bestanden.

Gekozen is voor cliënt-gestuurde ftp-sessies. Gelet op de betrekkelijke eenvoud levert dat in de praktijk nauwelijks problemen op.

Beveiligingsaspecten
Er is uiteraard aandacht besteed aan beveiligingsaspecten. Autorisatie op gebruikersniveau vindt plaats op de server.
Daarnaast is bestudeerd hoe verdergaande beveiliging in te voeren middels een VPN oplossing (met gebruik internettunneling en certificaten). Geëxperimenteerd is met VPN/tunnel-software (Checkpoint) waarbij op de cliënt

(PC veehouder) de tunnelsoftware wordt geïnstalleerd en aan de serverkant een serverversie van deze software. De tunnel zorgt voor encryptie van de data tussen zender en ontvanger, op deze manier kan een ftp-sessie volledig afgeschermd van de rest van internet geboden worden.

Alhoewel deze beveiligingsoptie als goed en afdoende wordt beschouwd wordt deze vooralsnog nog niet ingezet.

Logging en retourberichten
Logging wordt op (ftp-)sessie niveau op zowel de cliënt als ook op de server uitgevoerd.
Logginginformatie op het niveau van bericht, gebeurtenis (koenummer) is nog niet beschikbaar maar zal volgens AgiS beschikbaar moeten komen in de vorm van retourberichten. Daarbij wordt gepleit voor het terugsturen van elke gebeurtenismelding, de omvang van de EDI berichten doet er immers steeds minder toe als we kijken naar de communicatiegebruikskosten van internet.

Aandachtsgebieden / knelpunten
De volgende gebieden vragen om aandacht:

1. Invulling retourberichten
2. Aanscherping beveiligingsaspecten i.r.t. aanscherping eisen , bijvoorbeeld door I&R
3. Sturing van het proces van aanleveren data is bij Zuivelnet minder een hot-item vanwege de geringere kans op menselijke bedieningfouten en het aanbieden van een aangepaste ftp-schil. Toch zou nog kritisch nagedacht kunnen worden over:
   - Het verdere aanmoedigen of forceren van het gebruik van gegevensuitwisseling, rechtstreeks via het MIS (gestuurd).
   - Overwogen kan worden om gebruik te maken van servergestuurde communicatieprocessen waarbij bijvoorbeeld gebruik wordt gemaakt van een script welk steeds per sessie wordt gegenereerd op de server, wordt opgehaald door de cliënt en wordt uitgevoerd vanaf de cliënt.

Bijlage 7.3. KI-Samen en KI-Kampen

De verwerking van KI-berichten is vergelijkbaar met die van de DHZ-KI van het NRS. Gekozen is voor eenzelfde directorystructuur op de server en bestandsbeheer voor de verwerking.
Met betrekking tot de autorisatie (beveiliging) is er een groot verschil te bespeuren. Toegang is niet per gebruiker, met eigen toegangscodes, maar centraal voor alle gebruikers hetzelfde geregeld. Er is dus maar één gebruikersnaam en wachtwoord en deze is bij iedereen bekend. Het mag duidelijk zijn dat hiermee de beveiliging nauwelijks is geregeld en dat de kans niet is uitgesloten dat bestanden van verschillende veehouders elkaar kunnen overschrijven voordat ze verwerkt zijn.

Ook hier zijn de aandachtsgebieden zoals benoemd bij EDI-Zuivel van toepassing.

Bijlage 7.4. Netkoerier applicatie

Beheersorganisatie en structuur
NetKoerier® is een eenvoudig te bedienen commercieel programma van Rovecom, dat van begin tot eind de datacommunicatie verzorgt. Van het versturen van bestanden uit de juiste directory, tot het plaatsen van de gegevens in de juiste directory van de ontvangende computer. Daarbij kunnen ook andere opdrachten uitgevoerd worden, zoals het hernoemen en verwijderen van bestanden. Ter controle van het verloop van de communicatie wordt een ontvangstbevestiging vanuit de ontvangende computer voor de versturende partij gegenereerd.
Het NetKoerier® systeem is flexibel opgezet. Alle soorten bestanden kunnen worden verstuurd, zoals tekstbestanden, databases, etc. De cliënt versie kan met meerdere FTP-servers communiceren, zodat de gebruiker met meerdere organisaties informatie kan uitwisselen in een communicatie sessie.
Het systeem is uitermate geschikt voor een organisatie die regelmatig informatie uitwisselt met een (groot) aantal vaste relaties.

Met NetKoerier® wordt het communicatieproces door de server volledig aangestuurd door middel van scripts welke per sessie op de server worden gegenereerd. Deze worden opgehaald door de cliënt en worden uitgevoerd vanaf de cliënt.

Toepassingen

Operationeel:	FTP-NRS: melkcontrole naar Rantsoenvoorlichter van mengvoerbedrijf. Mestanalyses en –bonnen uitwisselen tussen intermediairs en laboratoria. Bestanduitwisselingen tussen applicaties.
Mogelijkheden:	EDI's, documenten etc. uitwisselen met één of meerder ftp-servers.

Beheer
Gedeeld beheer tussen de organisatie die data verstuurt/ontvangt en Rovecom.

Uitwisseling data door gebruiker/veehouder
- Vanuit het programma handmatig met één commando te bedienen. Programma verzorgt het ophalen, versturen en hernoemen van bestanden automatisch op basis van scripts.
- Aan te roepen door programma's van derden, bijvoorbeeld MIS.
- Automatisch ophalen van data van meerdere ftp servers in eenzelfde sessie. Op deze wijze worden menselijke fouten voorkomen.

Beveiligingsaspecten
- Authenticatie: via autorisatiescode voor een gebruiker op de NetKoerier® server
- Encryptie/versleuteling data: Secure Socket Layer Techniek
- Logging: op cliëntniveau en systeemniveau.

Aandachtsgebieden / knelpunten
- Kostenaspect ; elke cliënt moet worden voorzien van de NetKoerier cliënt software.
- Beveiliging: nu alleen nog op niveau van netwerkencryptie. Echt volwaardige authenticatie m.b.v sleutelparen c.q. certificaten is nog niet mogelijk.

Bijlage 8. Afspraken e-mail attachments (EAN + aanvullend EAV)

E-mail envelop

Content type
Deze MIME header wordt gebruikt om het type attachment aan te duiden. Deze type aanduiding kan door het computersysteem van de ontvangende partij worden gebruikt om de bijbehorende applicatie op te starten. Het voorgeschreven 'Content type' voor een EDIFACT bericht is: application/EDIFACT. Uit het procesoverzicht op pagina 28 blijkt echter dat beveiligde berichten eerst worden geëncrypt en gesigneerd en dat daarna pas de MIME headers worden aangebracht. In werkelijkheid bestaat het proces van versleutelen en signeren van een bericht uit een aantal stappen. Elke stap en elke type beveiliging kent zijn eigen 'Content type'. Voorbeelden van berichten die op deze manier zijn versleuteld kunt u vinden in het document: Requirements for Inter-operable Internet EDI en MIME-based Secure EDI op de website van de Electronic Data Interchange-Internet Integration werkgroep (http://www.ietf.org/html.charters/ediint-charter.html) Het 'Content type' van een beveiligd EDI-bericht is dus ook afhankelijk van de gebruikte beveiliging.

Aanvullend EAV: ***Content type=application/ADIS***
Voor ADIS bestanden bestaat geen content-type. Omdat er ruimte is voor vrije invulling wordt hier voorgesteld te werken met **Content type=application/ADIS.**

Conform de afspraken van de Electronic Data Interchange-Internet Integration (EDIINT) werkgroep mag naast de bodypart met de (beveiligde) EDI berichten geen andere type bodyparts in het bericht voorkomen. 'Lege' bodyparts of bodyparts met een begeleidende tekst zijn dus niet toegestaan. Dit soort bodyparts worden vaak wel gegenereerd bij het handmatig attachen van een bericht aan een e-mail pakket. In een attachment mag wel een interchange met meerdere EDIFACT berichten van verschillende typen voorkomen.

Tot slot is afgesproken dat er per E-mail bericht slechts één attachment mag worden gestuurd.

Aanvullend EAV: meerdere berichten
Meerdere berichten of bestanden zijn wel mogelijk maar moeten dan in één gecomprimeerd bestand worden geattached

Content-Transfer-Encoding
Ook de manier waarop de gegevens in een bericht worden gecodeerd in binaire tekens moet worden vastgelegd. In grote lijnen zijn de opties: 7BIT of Base64. De pilotwerkgroep heeft gekozen voor Base64 omdat 7BIT een UN/EDIFACT characterset van UNOC en hoger uitsluit en tevens een maximale regellengte van 74 tekens kent.

Subjectregel
Of er wat in de subjectregel moet worden ingevuld moet bilateraal worden afgesproken. De subjectregel mag echter niet worden gebruikt om een automatische verwerking mogelijk te maken. Hiervoor is immers de MIME Header 'content type' bedoeld. In de subjectregel kan bijvoorbeeld wel het EDI bericht type worden opgenomen om het zoeken aan een helpdesk te vergemakkelijk.

Naamgeving attachment
De naamgeving van de attachment wordt volledig vrijgelaten. Ook deze MIME header mag niet worden gebruikt om een automatische verwerking mogelijk te maken.

Naamgeving E-mail postbus
De naamgeving van de E-mail postbus waarmee de E-mail berichten worden ontvangen c.q. verzonden is vrij te kiezen door de organisatie die de postbus aanmaakt. Geadviseerd wordt om hierbij geen persoonsnamen te gebruiken omdat dit tot een misverstand kan leiden als de persoon in kwestie bijvoorbeeld van functie veranderd. Vanuit beheersmatig oogpunt is het sterk aan te bevelen om vanuit slechts een E-mail postbus berichten te sturen. Ook het inrichten van een specifieke postbus waarnaar alleen maar EDI E-mail attachment kunnen worden gestuurd is aan te bevelen. Deze infrastructuur moet zo stabiel mogelijk zijn en zo min mogelijk worden gewijzigd.

Aanvullend EAV: dedicated postbus
Sterk aanbevolen wordt een aparte postbus te reserveren voor EDI berichten, bij voorkeur onder de bedrijfsnaam (of zoveel als mogelijk herkenbaar). In principe moet worden voorkomen dat deze postbus ook voor andere dan EDI-verkeers doeleinden wordt gebruikt.
Tevens wordt sterk aanbevolen enkel met positief gereputeerde internet providers zaken te doen, bij voorkeur niet de aanbieders van gratis e-mail.
Er zal overigens geen lijst van 'preferred ISP's worden aangeboden.

Omvang E-mail berichten
Geadviseerd wordt de omvang van een E-mail bericht met een EANCOM attachment te beperken tot 2 Mb. Hierbij wordt gedoeld op de maximale grootte na encryptie bij verzenden c.q. voor decryptie bij ontvangst. Deze omvang is gebaseerd op de maximale omvang van een X.400 bericht. Het is namelijk mogelijk om E-mail attachments bij een ontvanger met een X.400 postbus af te leveren (en vica versa).

Aanvullend EAV: dedicated postbus
Deze afspraak lijkt arbitrair. De genoemde beperkingen met maximale berichtomvang worden wel in zijn algemeenheid onderkent maar worden niet herkend in de eigen X400 postbussystemen.
Het lijkt raadzaam de maximum grens in de praktijk, per toepasing (of b.v. gebruikersgroep) vast te stellen, de genoemde 2 Mb kan daarbij gelden als default waarde.

Beveiliging

Daar waar gesproken wordt over beveiliging wordt bedoeld het versleutelen van de informatie met de publieke sleutel van de ontvanger en het ondertekenen van het (versleutelde) bericht met de private sleutel van de verzender.

Berichten
Aanvullend EAV
Per gebruikersgroep zal bepaald moeten worden of berichten beveiligd verstuurd moeten worden. Bij het EDIFACT factuurbericht zal daar vrijwel zeker sprake van zijn.

Uitwisseling sleutels
Het uitwisselen van de sleutels kan via E-mail worden gedaan maar alleen na overleg met de ontvangende partij.

Naamgeving certificaat
Bij een sleutelpaar hoort ook altijd een certificaat. De naamgeving van dit certificaat wordt vrijgelaten.

Versie en sleutellengte S/MIME en PGP
De gebruikte beveiligingstechniek moet tenminste S/MIME v2 en PGP/MIME ondersteunen. Belangrijker is echter de sleutellengte. Vanuit beveiligingsoogpunt wordt de minimale sleutellengte vastgesteld op 1024 bits.

Aankomstbevestiging
EAN beveelt aan het EDIFACT APERAK bericht te gebruiken als ontvangstbevestiging.
Het APERAK bericht kan worden gebruikt om de ontvangst van elk berichttype te bevestigen. In onderling overleg moet worden bepaald welke berichten middels het APERAK bericht moeten worden bevestigd. Bewust is niet gekozen voor het gebruik van de op internet beschikbare bevestigingsberichten omdat er onvoldoende zekerheid aan kan worden ontleend.
Wel moet er rekening mee worden gehouden dat het implementeren van een APERAK bericht ingrijpende aanpassingen noodzakelijk kan maken. Bijvoorbeeld moet er mogelijk automatisch gereageerd worden op het uitblijven van een APERAK bericht.
Voor de definitie van het APERAK bericht zie pagina 40 (Bijlage UN/EDIFACT APERAK MESSAGE)

Aanvullend EAV
Omdat EAN geen ADIS berichten in beheer heeft doet zij daarover geen uitspraken. Geadviseerd wordt om voor ADIS berichten de ADIS gebeurtenis 'Ontvangstbevestiging' te gebruiken. Meer hierover in hoofdstuk 7 (Retour-/ bevestigingsberichten).