# Vertrouwen in de data-uitwisseling van STIS

Penners, L.J.T.M.

*Award date:*
2003

# Vertrouwen in de data-uitwisseling van STIS

| | |
|---|---|
| *Datum* | 7 augustus 2003 |
| *Vaknaam* | Afstudeeropdracht TEMA<br>Technische richting: Informatietechnologie<br>Studiestroom: Techniek & Beleid |
| *Naam* | ing. Léon Penners<br>L.J.T.M.Penners@student.tue.nl |
| *Studentnummer* | 443435 |
| *Opdrachtgever* | Ministerie van Verkeer en Waterstaat<br>Rijkswaterstaat Adviesdienst Verkeer en Vervoer |
| *Begeleider Rijkswaterstaat* | ir. Lea Kuiters<br>L.Kuiters@avv.rws.minvenw.nl |
| *1e Begeleider TU Eindhoven* | mr. dr. ir. ir. Lambèr Royakkers<br>L.M.M.Royakkers@tm.tue.nl |
| *2e Begeleider TU Eindhoven* | mr. drs. Ted Clarkson<br>E.F.Clarkson@tm.tue.nl |

## INHOUDSOPGAVE

## Lijst van figuren



## Lijst van tabellen

## WOORD VOORAF

Dit woord van dank richt ik aan de personen die een significante bijdrage hebben geleverd aan het tot stand komen van dit afstudeeronderzoek.

Allereerst mijn bewondering voor de voortdurende steun, die ik van mijn echtgenote Ilse Penners-Knoors heb ontvangen, gedurende de 6 jaar deeltijdstudie "Techniek en Maatschappij" aan de Technische Universiteit Eindhoven. Samen met onze zoon Daniek heeft ze moeten doorstaan, dat ik het laatste jaar van mijn opleiding regelmatig vrije tijd opofferde aan het afstudeerwerk.

Ir. Lea Kuiters van Rijkswaterstaat Adviesdienst Verkeer en Vervoer; toen ik haar benaderde voor een afstudeeronderwerp was zij onmiddellijk enthousiast in het meedenken over het onderzoek. Steeds wist ze ruimte in haar drukke agenda te creëren voor het doorlezen en bespreken van conceptrapporten. Tijdens deze besprekingen heb ik veel van haar geleerd over de Nederlandse binnenvaartsector. Zonder haar was dit onderzoek beslist moeizamer verlopen.

Mr. dr. ir. ir. Lambèr Royakkers heeft me als eerste begeleider van de Technische Universiteit Eindhoven steeds gestimuleerd om het kwaliteitsniveau van dit onderzoek verder te verbeteren. Ik kijk met plezier terug op de buitengewoon prettige samenwerking ten behoeve van mijn afstuderen.

Mr. drs. Ted Clarkson heeft als tweede begeleider van de Technische Universiteit Eindhoven me gestimuleerd door het kritisch beoordelen van de tussentijdse versies van dit rapport. De discussies tijdens de besprekingen gaven me steeds inspiratie tot het verbeteren van mijn betoog.

Verder richt ik mijn dank aan ir. Henk Verkerk, Bertha Verkerk, Peter Lousberg en Janine Hochstenbach. Samen met Ilse Penners waren zij zo vriendelijk hun opmerkingen en suggesties voor mij op schrift te stellen. Door de bijdrage van deze personen is de layout, de schrijfstijl en de opbouw van dit rapport aanmerkelijk verbeterd.

In de eindfase van het afstuderen heeft mijn collega ir. Henk Verkerk van Rijkswaterstaat De Maaswerken me meermaals weten te motiveren, zodat ik voldoende vaart wist te houden in mijn afstudeertraject.

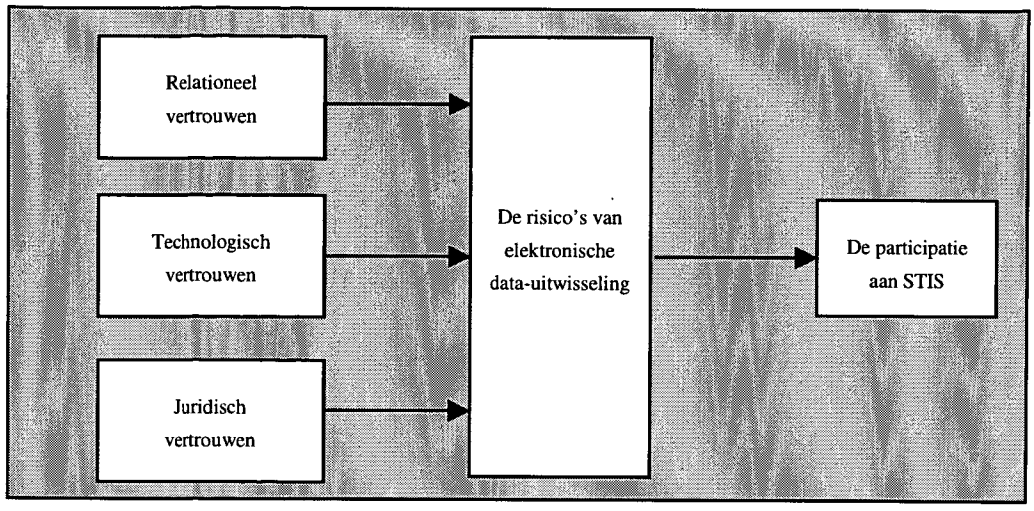
## SAMENVATTING

Het vervoer van goederen over de Nederlandse binnenwateren dient in de toekomst nog steeds veilig en vlot te verlopen. Het vervoer via schip kan een deel van het groeiende wegvervoer overnemen, mits de binnenvaartsector werkt aan een beter planbare scheepvaart. De scheepvaart wordt beter planbaar indien de actoren, welke actief zijn op het vlak van vervoersmanagement (commerciële ondernemingen) en het verkeersmanagement (voornamelijk overheid), gegevens naar elkaar gaan uitwisselen. Door de onderlinge data-uitwisseling kan de gezamenlijke inspanning voor het verwerven van deze informatie gereduceerd worden. De data-uitwisseling wordt geïmplementeerd door het project STIS (Scheepvaart Transport Informatie Services); een project waarbij Rijkswaterstaat Adviesdienst Verkeer en Vervoer de opdrachtnemer en het Ministerie van Verkeer en Waterstaat de opdrachtgever is.

Verwacht wordt dat de data-uitwisseling tussen een aantal partijen uit de binnenvaartsector niet soepel zal verlopen. Zonder aanvullende maatregelen vanuit STIS, ontbreekt het bij deze partijen aan vertrouwen voor de uitwisseling van deze gegevens. Dit onderzoek adviseert welke aanvullende maatregelen nodig zijn en welke partijen deze maatregelen moeten implementeren, om het vertrouwen in de data-uitwisseling van STIS te vergroten.
Bij de data-uitwisseling van STIS kunnen de volgende gevoeligheden voor de data-uitwisseling bestaan:

- **Privacygevoelige gegevens**
  Bij de registraties betreffende schip, lading, reis en opvarenden door middel van landelijk dekkende informatiesystemen, is de koppeling met persoonsgerelateerde gegevens vrij eenvoudig te realiseren. Deze registratie stimuleert de veiligheid en de vlotheid van het verkeer op de binnenwateren. De privacy van de schipper is hierbij in het geding.
- **Bedrijfsgevoelige gegevens**
  Bedrijfsgevoelige gegevens bevatten informatie over het operationeel of strategisch handelen van een commerciële onderneming uit de binnenvaartsector. Deze informatie kan door een andere partij uit de sector gebruikt worden om zijn concurrentiepositie te verbeteren ten kosten van de ene partij.
- **De kwaliteit van de nautische gegevens**
  Bij het on-line presenteren en het frequenter verversen van nautische informatie suggereert de verstrekker een grotere mate van nauwkeurigheid van deze gegevens. Voor deze gegevens bestaat het risico, dat ze niet correct zijn of worden weergegeven. De verstrekker van deze gegevens kan aansprakelijk gesteld worden in geval van schade, ontstaan door de verstrekking van onjuiste gegevens.
- **De status van de elektronische transactie**
  Bij het afsluiten van overeenkomsten via elektronische berichten ontbreekt een sluitend juridisch kader met betrekking tot: een geldige totstandkoming van de overeenkomst, de vormvereiste van de overeenkomst, het bewijs, de identiteit en de bevoegdheid van de afzender, de fouten in de berichtgeving en het bewaren van berichten.

Bij deze bovengenoemde gevoeligheden is er sprake van een gebrek aan 'vertrouwen'. De gevoeligheden in de data-uitwisseling worden gebundeld in het conceptuele model van STIS door de variabele 'risico's van de elektronische data-uitwisseling'. Deze risico's worden gereduceerd door het vergroten van het relationeel, technologisch en het juridische vertrouwen. Op basis van dit conceptuele model van STIS worden maatregelen gedefinieerd, welke de bovengenoemde vormen van vertrouwen positief beïnvloeden.




De geadviseerde maatregelen zijn gebundeld in de categorieën:

- Informatiebeveiliging;
- Opleiding en training;
- Interchange Agreement;
- Trusted Third Party;
- Aanpassingswet Elektronische Handel.

Per gevoeligheid worden maatregelen uit de bovengenoemde categorieën onderkend. Deze maatregelen beïnvloeden het vertrouwen in de data-uitwisseling van STIS positief. De implementatie van deze maatregelen wordt uitgevoerd door de regiegroep STIS, de Trusted Third Party en de grote commerciële en niet-commerciële deelnemende partijen aan STIS. Een beperkt aantal maatregelen wordt geïmplementeerd door de individuele schippers.

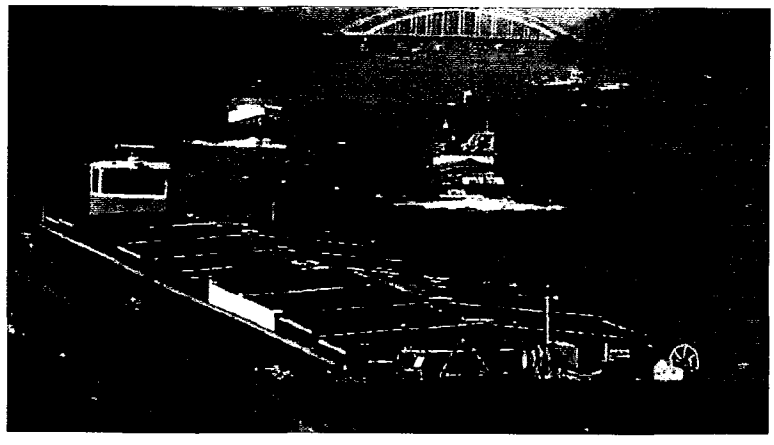
Rekening houdende met de STIS-implementatie voor het jaar 2005, is de volgende prioriteitenlijst aan te bevelen:

1. In overleg met relevante deelnemers aan STIS, overeenstemming bereiken over de inhoud van de Interchange Agreement op hoofdlijnen;
2. Het starten van een onderzoek naar het vereiste takenpakket van een Trusted Third Party binnen STIS;
3. Het starten van een onderzoeken naar het vereiste niveau van informatiebeveiliging in het kader van STIS.

# 1 Inleiding

De Nederlandse binnenvaartsector biedt voor het goederenvervoer tussen Nederland en de vele bestemmingen binnen (West-) Europa een veilig, milieuvriendelijk en efficiënt alternatief voor de nog steeds groeiende stroom van goederenvervoer over de weg.
In het Vaar-Plan 2001-2005 (V&W-1, 2001) wordt het beleid van Verkeer en Waterstaat verwoord hoe deze voordelen van de binnenvaart ondersteund kunnen worden door de inzet van telematica voor het verkeer en vervoermanagement.
De Nota "Varen in de digitale delta" (V&W-2, 2001) wijst op de mogelijkheden bij een efficiëntere data-uitwisseling tussen binnenvaartpartijen.

Op dit moment vindt er tussen een aantal partijen uit de binnenvaartsector reeds data-uitwisseling[1] plaats ten behoeve van het verkeers- of het vervoersmanagement. Door middel van mobiele telefonie, fax, PC en marifoon worden gegevens betreffende het schip, de (toekomstige) reis, de (toekomstige) lading, de toestand van de vaarweg, enz. doorgegeven aan belanghebbende partijen. Dit alles om de reis correct en soepel te laten verlopen, of een vracht op een efficiënte wijze aan te nemen. Herhaaldelijk worden daarbij dezelfde gegevens verstrekt aan de diverse partijen. Bij een gegevensoverdracht in gesproken of handgeschreven vorm is een onvolkomenheid snel geïntroduceerd.
De verschillende informatiesystemen in de binnenvaartsector kennen een lage graad van integratie. Hierdoor is het op dit moment onmogelijk bepaalde soorten van informatie (o.a. statistieken betreffende waterstanden en capaciteitscijfers van kunstwerken t.b.v. de planning van toekomstige reizen) te benaderen. Het project Scheepvaart Transport Informatie Services (STIS[2]) zal een optimalisatie



**Figuur 1-1: Binnenvaart op Nederlandse wateren.**

voor deze bovengenoemde situaties nastreven, via de implementatie van een efficiënte data-uitwisseling.
De binnenvaartsector functioneert op basis van een historisch opgebouwd rela-

[1] In dit onderzoek worden de begrippen 'data' en 'gegevens' gebruikt. De betekenis is identiek. Indien het begrip 'informatie' wordt toegepast, heeft dit de betekenis van *geïnterpreteerde data.* De transmissie van data, of gegevens wordt in dit rapport data-overdracht genoemd.
[2] Voor uitgebreide informatie betreffende het project STIS, zie www.stis.nl.

tienetwerk. De belangrijkste partijen in de binnenvaartsector zijn schippers, verladers en intermediairs. De groep binnenvaartschippers bestaat voor een groot deel uit eenpersoonsbedrijven. Ze verwerven hun vrachten via hun vaste contacten in het relatienetwerk, welke sterk gebaseerd is op vertrouwen tussen de partijen onderling. Tot op heden is de elektronische data-uitwisseling in de binnenvaartsector betreffende de vraag en aanbod naar goederen beperkt gebleven tot pilots, uitgevoerd door consortia van belangenverenigingen en ICT-/serviceproviders. Deze initiatieven zijn niet succesvol geweest. Indien partijen geen opties meer hadden in hun relatienetwerk werd het elektronische netwerk ingezet om ladingen aan te bieden. Binnen bestaande netwerken van schippers, reders, samenwerkingsverbanden en verladers worden er elektronische gegevens uitgewisseld (vaak via E-mail).
Een verbeterde (gestandaardiseerde) data-uitwisseling betreffende de vraag en aanbod van goederen kan een bedreiging zijn voor het relatienetwerk, ook al zou de marktwerking hierdoor kunnen verbeteren. De sociale functie van dit relatienetwerk en het bestaan van vele kleine partijen in de binnenvaartsector speelt hierbij een belangrijke rol. De drive om over te gaan tot een verbeterde data-uitwisseling (innovatie) is, zonder het nemen van aanvullende maatregelen, daarom relatief laag.

Voor de Nederlandse binnenvaartsector zal de data-uitwisseling, zoals die door STIS wordt nagestreefd, een bijdrage leveren aan een veiliger, vlotter en beter planbare scheepvaart. De veiligheid voor de scheepvaart wordt verbeterd, aangezien meer details bekend worden t.a.v. gevaarlijke ladingen. De vlotheid van de scheepvaart zal verbeteren, aangezien het herhaaldelijk uitwisselen van gegevens via conventionele communicatiesystemen relatief veel tijd vergen. De planbare scheepvaart wordt haalbaar, aangezien een aantal gegevens (meteo, stremmingen, waterstanden, enz.) geïntegreerd gaan worden, welke een compleet beeld geven van de toestand van de vaarroute, voor aanvang van een reis. Dit totaalpakket aan verbeteringen is de winst die gezamenlijk voor bedrijfsleven en overheid te behalen is.

## 1.1 STIS en de aanleiding van het onderzoek

In Europees verband is het innovatieprogramma RIS (River Information Services) opgestart. RIS zal uiteindelijk een groot deel van de Europese binnenwateren voorzien van een efficiënte informatie-infrastructuur, ter ondersteuning van het vervoer van goederen over de binnenwateren. Het Ministerie van Verkeer en Waterstaat heeft aan Rijkswaterstaat Adviesdienst Verkeer en Vervoer de opdracht gegeven het RIS-concept te vertalen naar de Nederlandse situatie. Dit initiatief heeft de naam Scheepvaart Transport Informatie Services (STIS) gekregen. Daarmee wordt het in de inleiding geformuleerde beleid vertaald naar maatregelen.

Het project(-resultaat) van STIS vertoont de volgende kenmerken (AVV-1, 2001):

- **STIS als samenwerking in de binnenvaartsector, gestoeld op informatie- en communicatietechnologie.**
  In het project STIS wordt door de overheid en het bedrijfsleven samengewerkt, zodat de volgende gemeenschappelijke doelen worden nagestreefd:
  - de versterken van de veiligheid van binnenvaart;
  - het vergroten van de flexibiliteit van de binnenvaart;

➢ het beter benutten van de beschikbare infrastructuur.
De huidige stand van de ICT wordt daarbij als uitgangspunt genomen. Een intensieve betrokkenheid van de partijen uit de binnenvaartsector is een voorwaarde voor het laten slagen van dit innovatietraject.

- **STIS is geen nieuw systeem, maar een gemeenschappelijke omgeving voor bestaande systemen en werkprocessen.**
  Vanuit de STIS gedachte zijn de benodigde taken en functies in een inventarisatieronde door deelnemende partijen uit de binnenvaartsector in kaart gebracht. Op deze wijze is een gerichte informatiearchitectuur bepaald volgens welke de data-uitwisseling efficiënter kan gaan plaatsvinden. STIS is niet zozeer één systeem, maar een gemeenschappelijke omgeving waarbinnen door verschillende partijen meerdere systemen worden ontwikkeld, die onderling data kunnen uitwisselen. Daarbij wordt optimaal gebruik gemaakt van bestaande systemen en werkprocessen.

Door een grote groep experts, allen direct betrokken bij de scheepvaart, is gewerkt aan deze vertaling van RIS naar de Nederlandse situatie. In de loop van het jaar 2001 en 2002 is door deze groep van experts de architectuur van STIS beschreven. Bij het maken van deze beschrijving kwamen vanuit de groep toekomstige gebruikers van STIS signalen dat er een gebrek aan vertrouwen bestond ten aanzien van de data-uitwisseling volgens STIS.
Uit aanvullende interviews met deskundigen betreffende de binnenvaartsector (Kuiters-Goederen, 2002) is geconstateerd, dat er een gebrek aan vertrouwen wordt verwacht ten aanzien van de data-uitwisseling. In de informatiearchitectuur van STIS (AVV-2, 2001) is deze uitwisseling van data beschreven. Voor data-uitwisseling van de volgende soorten gegevens wordt verwacht, dat er een gebrek aan vertrouwen bestaat:

- Aangezien het grootste deel van de binnenvaartschippers eenpersoonsbedrijven (particuliere ondernemers) vormen, kan vanuit de scheepsregistraties eenvoudig de locatie van deze personen afgeleid worden; dit vormt een bedreiging voor de privacy van deze groep schippers;
- In de binnenvaart bestaat een aantal terminalbeheerders, welke tevens de rol van vlootbeheerder vervult. Aanvullend daarop maken deze terminalbeheerders gebruik van schepen van particuliere ondernemingen (eenpersoonsbedrijven). Deze terminalbeheerders hebben hierdoor een goed inzicht in de operationele gegevens van deze eenpersoonsbedrijven. Voor de efficiënte bedrijfsvoering van zijn eigen terminal, kan de terminalbeheerder de operationele gegevens van deze eenpersoonsbedrijven misbruiken. Dit gaat ten koste van de kleine ondernemer. De terminalbeheerder gebruikt de particuliere onderneming voor het opvangen van de pieken in zijn logistieke planning.
- De vaarwegbeheerders hebben meetnetten in gebruik, waarmee actuele nautische[3] en waterstandsgegevens worden verzameld. De vaarwegbeheerders zijn tot op heden steeds terughoudend geweest met het verstrekken van deze meetgegevens aan de vaarweggebruikers. Indien een schade is ontstaan als gevolg van de interpretatie van de verstrekte gegevens zou de vaarwegbeheerder een aansprakelijkheidsrisico kunnen lopen. De veiligheidsmarges en de frequentie van verstrekking worden daarom tot op heden vrij groot gehouden om het risico van aansprakelijkheid zo klein mogelijk te houden. De vaarwegbeheerder kon zich daarbij steeds beroepen op de scheepvaartverkeerswet, waarbij de schipper steeds zelf dient te bepalen of een lokale

[3] nautische: tot de scheepvaart behorend.

situatie geen risico vormt voor zijn vaartuig. Hiermee blijft de schipper zelf aansprakelijk in haast alle voorkomende situaties op de vaarweg.
De data-uitwisseling van STIS geeft de vaarweggebruikers real-time toegang tot nautische en waterstandsgegevens. Hiermee zal de vaarwegbeheerder de indruk wekken, dat de kwaliteit van de nautische gegevens hoger is dan in het verleden. Door de vrije toegang tot deze actuele data zal de aansprakelijkheidspositie voor de vaarwegbeheerder verslechteren in het geval van schades ten gevolge van de verstrekking van onjuiste gegevens;

- Bij het uitwisselen van data langs elektronische weg worden ten behoeve van het vervoer van lading (tussen vervoerders, verladers, expediteurs, terminalbeheerders, enz.) overeenkomsten aangegaan. Dit is een efficiënte manier van zaken doen. Maar zodra de partijen het niet eens zijn over de afwikkeling van de overeenkomst, bevat de wetgeving betreffende de elektronische handel een aantal grijze gebieden. Voor deze grijze gebieden is niet omschreven, hoe de verantwoordelijkheden liggen tussen de partijen die een overeenkomst langs elektronische weg afsluiten. Zou de overeenkomst op de traditionele manier zijn afgesloten, dan zou voldoende jurisprudentie voorhanden zijn om snel uit de impasse te komen. De grijze gebieden ontstaan daar, waar de elektronische overeenkomst nieuwe fenomenen introduceert ten opzichte van de conventionele overeenkomst. De jurisprudentie van de conventionele overeenkomsten voorziet dan niet in dit specifieke aspect welk typisch is voor de elektronische overeenkomst. Een voorbeeld hiervan is een gebrek in de berichtgeving. Een elektronisch bericht kan verminkt of verdwaald raken bij verzending. Indien dit gebrek niet wordt opgemerkt door de verzender of de (bedoelde) ontvanger kunnen juridische vragen ontstaan waar geen antwoord voor is vanuit de wetgeving of jurisprudentie.

De partijen kunnen door al deze gevoelige aspecten van de data-uitwisseling terughoudend zijn in de deelname aan de implementatie van STIS. Indien voor de genoemde aspecten onvoldoende vertrouwen bestaat zullen partijen niet deelnemen, hetgeen een bedreiging vormt voor de doelstelling van het project STIS. Het centrale begrip voor dit onderzoek is "vertrouwen". Specifiek handelt het hier om het soort vertrouwen dat er kan bestaan tussen organisaties onderling; ook wel inter-organisationeel vertrouwen genoemd. In paragraaf 2.3 wordt een selectie gemaakt uit de beschikbare definities van het begrip vertrouwen. Daaruit zal blijken dat de definitie van Dyer en Chu (Ratnasingam, 2001) het best past voor dit onderzoek. Vertrouwen is:

> *"De overtuiging van de ene partij, dat de andere partij in de uitwisselingsrelatie, haar kwetsbaarheid niet zal uitbuiten."*

Een tweede begrip dat voor dit onderzoek belangrijk is de "data-uitwisseling". De uitgewisselde gegevens, gebruikt om het verkeer en het vervoer efficiënter af te wikkelen, worden op een gestandaardiseerde wijze uitgewisseld. In paragraaf 1.3.3 wordt voor dit onderzoek afgebakend welk type van elektronische data-uitwisseling van toepassing is voor STIS.

In dit rapport wordt ingegaan op de data-uitwisseling waarbij een aantal gevoeligheden kunnen bestaan. Rond deze gevoeligheden in de data-uitwisseling is voldoende vertrouwen nodig, waardoor bij de deelnemende partijen het draagvlak ontstaat voor STIS.

## 1.2 De onderzoeksvragen

### *1.2.1 De doelstelling*

De leiding van het project STIS heeft opdracht gegeven voor het uitvoeren van een onderzoek naar de bedreigingen (zie paragraaf 1.1) voor de doelstelling van STIS. Het project STIS heeft de volgende doelstelling: "*Een succesvolle implementatie van de STIS-architectuur*". De doelstelling van dit onderzoek is rechtstreeks afgeleid van de projectdoelstelling van STIS en luidt:

> *"Een bijdrage leveren aan STIS, zodat de implementatie succesvoller zal verlopen, middels een gerichte inzet van de daarvoor geschikte instrumenten".*

Uit deze doelstelling worden de begrippen 'succesvol' en 'geschikte instrumenten' toegelicht.

De implementatie van STIS mag succesvol worden genoemd, indien alle relevante partijen uit de binnenvaartsector op elektronische wijze gegevens met elkaar gaan uitwisselen. Dit is het ideale eindresultaat voor het project STIS.

Het begrip 'geschikt instrument' wordt hier ruim geïnterpreteerd. Dit kan betrekking hebben op o.a. organisatorische, juridische, technische of financiële instrumenten. In de volgende hoofdstukken van dit rapport wordt bepaald welke van deze instrumenten een bijdrage aan de doelstelling kunnen leveren. Welke instrumenten geschikt zijn volgt uit een literatuurstudie betreffende het onderwerp vertrouwen in een omgeving van elektronische data-uitwisseling.

Het doel van dit onderzoek is maatregelen te vinden die een grote participatiegraad in STIS realiseren. Het effect van de maatregelen wordt gemeten door het registreren van de intentie van deelname bij de potentiële deelnemers, ten opzichte van een nulmeting. Deze nulmeting wordt uitgevoerd voorafgaande aan de implementatie van de geadviseerde maatregelen; de nulmeting zal worden uitgevoerd in de vorm van een enquête.

### *1.2.2 De probleemstelling*

Zoals in de inleiding aangeduid, is in samenspraak met de projectleiding van STIS de probleemstelling voor dit onderzoek geformuleerd. Uit voorgaande paragraaf blijkt, dat de participatiegraad aan STIS een relatie heeft met het vertrouwen in de data-uitwisseling van STIS. Uit literatuurstudie blijkt, dat het vergroten van het vertrouwen mogelijk is door gerichte inzet van maatregelen. De probleemstelling voor dit onderzoek luidt daarom als volgt:

> *"Welke maatregelen vergroten het vertrouwen in de data-uitwisseling van STIS?"*

Allereerst zal in kaart gebracht moeten worden, welke factoren van invloed zijn op dit gebrek aan vertrouwen in deze data-uitwisseling. Zodra deze factoren in beeld zijn, kunnen doeltreffende maatregelen worden ingezet om dit gebrek aan vertrouwen te voorkomen. Aangezien er ook data-uitwisseling plaatsvindt tussen verschillende typen van organisaties in andere branches, zal gezocht worden naar vergelijkbare situaties, waarbij maatregelen zijn ingezet tegen een dreigend

gebrek aan vertrouwen in data-uitwisseling. De deelvragen die hierbij gesteld kunnen worden luiden:

1. Wat is de gehanteerde definitie van vertrouwen? (Paragraaf 2.2)
2. Welk model voor vertrouwen is hier van toepassing? (Paragraaf 2.4)
3. Welk soort maatregelen vergroten het vertrouwen? (Paragraaf 3.1, 3.2, 3.3, 3.4 en 3.5)
4. Welke maatregelen worden voor STIS geadviseerd? (Paragraaf 4.1)

In de genoemde paragrafen van dit onderzoek zullen de antwoorden voor deze deelvragen uitgewerkt worden.

## 1.3 De kaders van dit onderzoek

Voor een nauwkeurige afbakening van het onderzoeksgebied worden in deze paragraaf de kaders van dit onderzoek aangegeven. De kaders hebben betrekking op geografie, de afbakening binnen de scheepvaartsector, de typering van elektronische data-uitwisseling en de rollen van de deelnemende partijen in STIS.

### *1.3.1 De afbakening naar geografie*

Het project STIS richt zich op de implementatie van STIS binnen Nederland. Dit bepaalt automatisch met welke wetgeving, telecommunicatie-infrastructuur, verkeersinfrastructuur, en binnenvaartorganisaties we te maken kunnen krijgen.

STIS streeft naar een deelname aan de data-uitwisseling door de relevante partijen uit de Nederlandse binnenvaartsector. Buitenlandse ondernemingen uit de binnenvaartsector (waaronder schippers) zullen in de toekomst geconfronteerd worden met een elektronische vorm van data-uitwisseling met betrekking tot het verkeer en het vervoer over de Nederlandse binnenwateren. Voor deze deelnemers aan de binnenvaart is er steeds een data-uitwisseling op conventionele wijze mogelijk. Dit in verband met het grensoverschrijdende karakter van het binnenvaartverkeer.

Het project STIS is een eerste uitwerking van het Europese RIS-concept. De STIS-architectuur en het referentiemodel van de scheepvaart, zoals ontwikkeld binnen STIS, zullen als blauwdruk gaan dienen voor de implementatie van het RIS-concept in een aantal andere Europese landen met binnenvaart. Op Europees niveau is door alle relevante lidstaten de intentie uitgesproken, dat ze voor 2005[4] een "River Information Service" (RIS) opzetten.

Vanwege de geografische afbakening wordt op het gebied van de wetgeving uitsluitend ingegaan op de Nederlandse wetgeving. Daar waar Europese regelgeving nog niet geïmplementeerd is in de Nederlandse wetgeving, zal ook de Europese regelgeving speciale aandacht krijgen.

STIS baseert zich op de huidig beschikbare telecommunicatie-infrastructuren, welke in Nederland geëxploiteerd worden (vast of draadloos). Daarmee wordt niet gekozen voor een communicatie-infrastructuur welke nog niet voldoende rijp (b.v. UMTS) is. De introductie van onvoldoende ontwikkelde communica-

[4] Deze doelstelling is geformuleerd in de "Declaration of Rotterdam" opgesteld tijdens de Pan-Europese Binnenvaartconferentie, gehouden op 5 en 6 september 2001 te Rotterdam. http://www.ivr.nl/nl/nl_declaratie-nl.htm

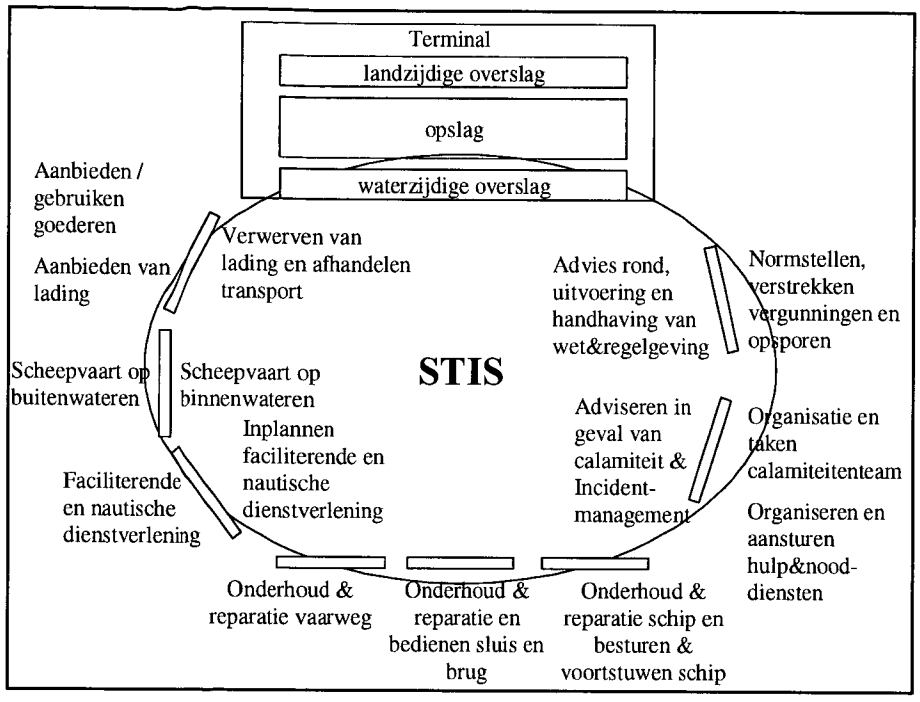
tie-infrastructuren zou een additioneel risico voor een succesvolle implementatie kunnen vormen.

De rollen en maatregelen uit dit onderzoek passen uitsluitend op de Nederlandse binnenvaartsector. Voor de implementatie van STIS in de andere Europese landen zullen er op detailniveau wijzigingen kunnen optreden in het gehanteerde referentiemodel voor de scheepvaart (AVV-1, 2001).

### *1.3.2 De afbakening binnen de binnenvaartsector*

De focus van STIS ligt op de vaarweg en haar raakvlakken met de wal en de zee. Vanuit het binnenvaartproces gezien bestaat de context voor STIS uit (Figuur 1-2):

- Landzijde – STIS reikt tot aan de opslag op een terminal. Via de terminal kan STIS worden opgehangen in een intermodale architectuur. De opslag op de terminal en landzijdige overslag vallen buiten de scope van STIS;
- Zeezijde – STIS dekt de scheepvaart op de binnenwateren af en daarmee de vaarwegen in zeehavens, in estuaria en over meren. De toegangsgeulen op zee en de zeevaart zelf vallen buiten de scope van STIS, echter de zeeschepen welke als verkeersdeelnemer de binnenwateren bevaren zijn wel van belang voor STIS;
- Lading – STIS begint bij het bevrachten van een schip of vloot van schepen en eindigt bij het afleveren van de goederen en afhandelen van het transport. De voorafgaande en daaropvolgende transportlogistieke handelingen vallen buiten de scope van STIS;
- Schip – STIS reikt tot aan het plannen van het onderhoud van het schip. Het uitvoeren van onderhoudswerkzaamheden valt buiten de scope van STIS. Wat betreft het fysieke transport reikt STIS tot en met de navigatie. De feitelijke besturing en voortstuwing van het schip vallen buiten de scope van STIS;
- Vaarweg – STIS richt zich op het gebruik van de vaarweg door het scheepvaartverkeer en de eventueel daaruit voortkomende incidenten en calamiteiten. Daarbij worden eventuele stremmingen door werk-in-uitvoering of beschadigingen aan de vaarweg meegenomen. De onderhouds- of reparatiewerkzaamheden vallen buiten de scope van STIS;
- Sluis – STIS richt zich op het veilig en vlot schutten van schepen. Het operationele bedienen van de sluizen valt buiten de scope van STIS, echter het gehanteerde beleid ten aanzien van bediening van de sluis is weer wel een punt van aandacht;
- Brug - STIS richt zich op het veilig en vlot laten passeren van schepen in relatie tot het verkeer op de weg. Het bedienen van de bruggen valt buiten de scope van STIS. Eveneens buiten de scope van STIS valt het verkeersmanagement op de weg. De brug vormt de schakel tussen verkeersmanagement op het water en op de weg;
- Dienstverlening – Het uitvoeren van de dienstverlening op en langs de vaarwegen aan de scheepvaart valt buiten de scope van STIS. Een voorbeeld hiervan is het bunkeren van proviand.




**Figuur 1-2: De context van STIS.**

### *1.3.3 De typering van de elektronische data-uitwisseling*

In elektronische data-uitwisseling bestaan verscheidene typen. Het type data-uitwisseling dat bij STIS wordt toepast, bouwt voort op de data-uitwisseling van een aantal bestaande systemen uit de binnenvaart. De bestaande systemen in de binnenvaartsector kenmerken zich door een EDI-achtige wijze van data-uitwisseling. Ook STIS vertoont de kenmerken van een data-uitwisseling op basis van EDI door:

- een bepaalde connectiviteit;
- een gestandaardiseerde berichtuitwisseling;
- een compatibiliteit met de berichten van bestaande systemen;
- een set van geformaliseerde afspraken;
- de relaties tussen de deelnemende partijen.

Voor het begrip EDI hanteren we binnen dit onderzoek de volgende definitie (Vlist et. al., 1994):

> *"EDI is de geautomatiseerde, elektronische uitwisseling van gestructureerde en genormeerde berichten tussen computers van verschillende organisaties."*

Volgens Van Esch kan EDI worden beschouwd als een specifieke vorm van E-commerce. Voor EDI bestaat er een onderverdeling in open en gesloten EDI. Dit heeft betrekking op de connectiviteit voor gebruikers (Esch, 1999). Sinds de introductie van het begrip Internet bestaan er 2 varianten EDI: gesloten en open EDI.

**Figuur 1-3: Een binnenvaartschip in contact met een verkeerspost.**

Gesloten EDI maakt gebruik van een afgeschermde technische omgeving en is niet te benaderen voor niet aangesloten deelnemers. Tussen de deelnemende partijen is doorgaans sprake van een overeengekomen contract (Interchange Agreement). De beslotenheid brengt met zich mee, dat de beveiliging van de informatiesystemen en de juridische zekerheid minder discussie oplevert dan bij open EDI. Nadeel van deze beslotenheid zijn de hogere investeringen voor de exploitatie (of huur) van het netwerk. Daarnaast kan bij gesloten EDI een eigen berichtenstandaard gehanteerd worden, welke uitsluitend bekend is bij de aangesloten deelnemers. Dit vergt een extra investering in specifieke informatiearchitecturen. De overstapkosten naar een andere EDI-standaard van data-uitwisseling zijn vrij hoog. Grote en sterke partijen in een bepaalde productieketen zetten gesloten EDI vaak in als strategisch middel, om een sterke binding te realiseren met zwakkere leveranciers of afnemers in de keten. De zwakkere partijen kunnen daardoor moeilijk overstappen naar een andere productieketen met een andere datastandaard, aangezien daarmee hoge investeringen gemoeid zijn.

Open EDI maakt gebruik van openbare netwerken, welke relatief goedkoop in het gebruik zijn. Vaak wordt gebruik gemaakt van het Internet. De servicekosten en exploitatie van Internet zijn relatief goedkoop. Om de openheid verder te bevorderen kan een open datastructuur voor EDI worden gehanteerd, welke (wereldwijd) gestandaardiseerd is voor de betreffende branche. Voor logistieke processen bestaan EDI-datastructuren of XML-definities (eXtensible Mark-up Language), welke wereldwijd toegepast worden.
Deze openheid vraagt extra aandacht voor de beveiliging van de data-infrastructuur.

Op dit moment lijkt voor STIS de keuze voor open EDI de meest voor de hand liggende; aangezien de huidige technieken voor de informatiebeveiliging betrouwbaar gebleken zijn, kan gekozen worden voor de goedkope dataverbindingen van het Internet.

Internationaal is er ter bevordering van het gebruik van EDI een verzameling regels ontwikkeld onder de naam EDIFACT. Deze regels worden door een groot aantal landen geaccepteerd als de standaard voor het uitwisselen van berichten door middel van EDI. Deze standaardisatie maakt het mogelijk de data-uitwisseling zelfs internationaal op éénduidige wijze te organiseren.

### *1.3.4 De typen van deelnemende partijen*

STIS omvat een zestal werkvelden. Binnen deze werkvelden wordt door verschillende partijen een aantal rollen ingevuld voor het functioneren van het betreffende werkveld. In onderstaande tabel worden de meest relevante rollen uit elk van de werkvelden genoemd. In dit rapport kan verwezen worden naar een bepaalde rol uit de binnenvaartsector. In onderstaande tabel wordt getoond welke organisatie welke rol vervult. In Bijlage 3 van dit rapport bevinden zich de definities van de rollen.

| Werkveld | Rol | Organisatie |
|---|---|---|
| **Vervoersmanagement en reisplanning** | Gezagvoerende schipper | Bedrijf |
| | Expediteurs aanbod / vraag | Bedrijf |
| | Vrachtbemiddelaar | Bedrijf |
| | Stuwadoor | Bedrijf |
| | Bemanning | Bedrijf |
| | Vlootbeheerder | Bedrijf |
| **Haven- en terminalplanning** | Gezagvoerende schipper | Bedrijf |
| | Terminalbeheerder | Bedrijf |
| | Havenbeheerder | Overheid |
| **Verkeersmanagement** | Gezagvoerende schipper | Bedrijf |
| | Vaarwegbeheerder | Overheid |
| | Havenbeheerder | Overheid |
| | Gezagvoerende schipper | Overheid |
| | Navigatie ondersteunende dienst | Overheid |
| | Sluismeester | Overheid |
| | Verkeersbegeleider op verkeerspost | Overheid |
| | Objectbedienaar | Overheid |
| **Handhavende taken** | Gezagvoerende schipper | Bedrijf |
| | Politie | Overheid |
| | Havenbeheerder | Overheid |
| | Rijksverkeersinspectie | Overheid |
| | Scheepvaartverkeersinspectie | Overheid |
| | Douane | Overheid |
| | Marechaussee | Overheid |
| | Rijkswaterstaat | Overheid |
| **Incidenten en calamiteiten** | Gezagvoerende schipper | Bedrijf |
| | Politie | Overheid |
| | Brandweer | Overheid |
| | Hulpdienst | Overheid |
| | Rijkswaterstaat | Overheid |
| | Waterschappen en polderdistricten | Overheid |
| **Statistiek** | CBS | Overheid |
| | Rijkswaterstaat | Overheid |

**Tabel 1-1: Rollen binnen STIS, ingevuld door overheden en bedrijfsleven.**

# 2 Het vertrouwen bij data-uitwisseling

## 2.1 Inleiding

STIS beoogt een data-uitwisseling te realiseren tussen informatiesystemen van de diverse deelnemende partijen, waarmee het vervoersmanagement (van particuliere organisaties) en het verkeersmanagement (de taak van overheidsorganisaties) beiden een efficiencywinst kunnen behalen. Bij data-uitwisseling voor deze soorten van relaties wordt door adviseurs betreffende de binnenvaartsector voorzien, dat er voor een aantal aspecten sprake is van een gebrek aan vertrouwen (Kuiters-Goederen, 2002).

In paragraaf 2.2 wordt allereerst bepaald welke definitie van vertrouwen voor dit onderzoek wordt toegepast.
De voorbereidende projectfasen van STIS hebben geleid tot een set van afspraken tussen deelnemende partijen aan STIS, betreffende de wijze van data-uitwisseling. Diverse partijen uit de binnenvaartsector wisselen al vele jaren data met elkaar uit. Maar voor een aantal partijen uit de binnenvaartsector is data-uitwisseling een nieuw fenomeen.
Indien deze partijen voor het eerst gevoelige data met elkaar gaan uitwisselen, zal er niet gelijk een basis van vertrouwen bestaan. Ze zullen zich afvragen of de data met voldoende voorzichtigheid worden behandeld. Vooral bij deze prille samenwerkingsvormen zal het motto zijn: "Dit vertrouwen zal moeten groeien".

In paragraaf 2.3 wordt een model samengesteld, waarmee het gebrek aan vertrouwen in STIS beschreven kan worden.
Na bestudering van diverse theorieën met betrekking tot elektronische data-uitwisseling in relatie tot vertrouwen, blijkt dit vertrouwen verschillende dimensies te hebben.

In paragraaf 2.4 wordt het conceptuele model van STIS geconfronteerd met de kenmerken van STIS.

## 2.2 De definitie van vertrouwen

In dit onderzoek is het begrip 'vertrouwen' al enkele malen gehanteerd, zonder de herkomst van de definitie te geven. Met de implementatie van STIS, zal een groot aantal partijen uit de Nederlandse binnenvaartsector intensief met elkaar gaan samenwerken ten aanzien van de data-uitwisseling. Dit onderzoek richt zich op het vertrouwen, dat van toepassing is op de relaties tussen de deelnemende partijen van STIS.

Gebruikmakend van de literatuur blijken er veel definities van 'vertrouwen' te bestaan. In haar proefschrift heeft Ratnasingam een uitgebreide inventarisatie gemaakt van verschillende definities van vertrouwen (Ratnasingam, 2001). De verschillende definities van vertrouwen komen voort uit studies betreffende verschillende disciplines, o.a. psychologie, management, sociologie, informatie systemen en management en marketing. In Bijlage 2 van dit onderzoek wordt de door haar verzamelde lijst van definities van vertrouwen weergegeven, welke van toepassing kunnen zijn. Voor het bepalen van de meest geschikte definitie

voor dit onderzoek, wordt een aantal selectiecriteria gehanteerd. In de onderstaande opsomming van deze (vetgedrukte) selectiecriteria wordt steeds aangegeven welke definities niet van toepassing zijn voor dit onderzoek:

- **Niet uitsluitend voor handelsrelaties**
  De data-uitwisseling van STIS beperkt zich niet tot de handel. Een aantal definities uit de inventarisatie van Ratnasingam zijn specifiek voor partijen die handel drijven met elkaar. Door een aantal deelnemers van STIS zullen langs elektronische weg contracten afgesloten worden; maar een groot aantal partijen zal zich beperken tot de uitwisseling van niet-commerciële informatie. Vanwege dit selectiecriterium passen de definities van Ganesan (*"De bereidheid zich met vertrouwen te verlaten op een handelspartner."*) en Zucker (*"Een set van logische verwachtingen, gedeeld door alle partijen, betrokken bij een economische uitwisseling."*) niet.
- **Kwetsbaarheid**
  Bij vertrouwen is er sprake van kwetsbaarheid. De ene partij die vertrouwen heeft in een andere partij stelt zich kwetsbaar op, zonder dat de ene partijen kan controleren of de andere partij zich gedraagt als verwacht. De ene partij loopt een risico. Binnen STIS worden data uitgewisseld, waarna de leverancier van deze data niet meer kan volgen hoe deze data verder verwerkt worden. Er moet een overtuiging bestaan dat de behandeling van de data op een juiste wijze gebeurd.
  Doordat het aspect kwetsbaarheid niet expliciet vermeld wordt vallen weer een aantal definities af, zoals b.v. Ring & Van de Ven (*"Vertrouwen als overtuiging voor de ene partij, omvat het verwachte gedrag en de loyaliteit van de andere partij."*) of Morgan en Hunt (*"Vertrouwen bestaat indien de ene partij overtuigd is van de betrouwbaarheid en integriteit in een uitwisselingsrelatie"*).
- **Vertrouwen is uni-directioneel**
  Het vertrouwen dat de ene partij in de andere partij heeft, hoeft niet wederzijds te zijn. Vele partijen in STIS zullen uitsluitend data leveren, terwijl ze nooit data zullen ontvangen. De leverende partij zal er dus van overtuigd moeten zijn dat de andere partij(-en) de kwetsbaarheden niet zal (zullen) uitbuiten.
  De definitie van Barney & Hansen (*"De wederzijdse overtuiging, dat geen van de partijen in een ruil, voordeel zal willen halen uit de ander zijn kwetsbaarheden."*) is daarom voor STIS niet van toepassing.
- **Overtuiging**
  De ene partij moet 'overtuigd zijn' van het vertrouwen. Dit is sterker uitgedrukt dan 'bereid zijn'. De definities, welke het aspect 'overtuiging' niet beschrijven vallen af voor dit onderzoek, bijvoorbeeld Mishra (*"De bereidheid van de ene partij om zich kwetsbaar op te stellen tegenover een ander partij, ervan uitgaande, dat de ander partij competent, open, betrokken en vertrouwelijk is."*)

Op basis van de bovengenoemde selectiecriteria, waaraan de definitie voor vertrouwen moet voldoen, resteert er voor dit onderzoek nog maar één bruikbare definitie uit de inventarisatie van Ratnasingam. De definitie van vertrouwen, opgesteld door Dyer en Chu omvat alle bovengenoemde eisen. Deze definitie luidt:

> *"De overtuiging van de ene partij, dat de andere partij in de uitwisselingsrelatie, haar kwetsbaarheid niet zal uitbuiten."*

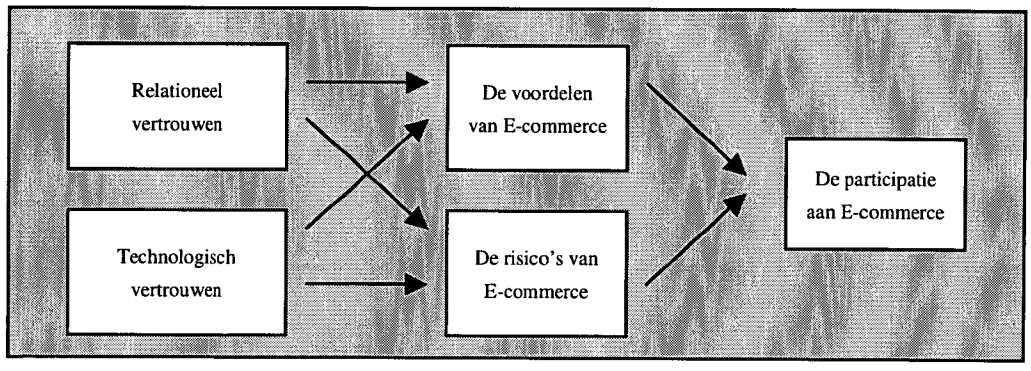
In deze definitie zijn de volgende termen essentieel: overtuiging, ene partij ten opzichte van de andere partij, uitwisselingsrelatie en kwetsbaarheid. Daarmee voldoet de definitie van Dyer en Chu aan alle bovengenoemde criteria; daarmee is deze definitie voor de data-uitwisseling binnen STIS toepasbaar.

## 2.3 Het model voor het onderzoek

Voor dit onderzoek zijn modellen gezocht, welke het verband inzichtelijk maken tussen vertrouwen in een inter-organisationele relatie en de variabelen die van invloed zijn op de mate van dit vertrouwen. In de literatuur zijn voor dit aandachtsgebied een aantal modellen te vinden. Net zoals bij de definitie van 'vertrouwen', zijn niet alle modellen van vertrouwen toepasbaar voor dit onderzoek.
In deze paragraaf wordt een geschikt model voor dit onderzoek geselecteerd. Een aantal criteria, die we bij de selectie van de definitie van vertrouwen reeds hebben toegepast, zal ook bij de modelselectie een rol van betekenis spelen:

- **Niet uitsluitend voor handelsrelaties.**
  Het model van vertrouwen is niet uitsluitend van toepassing op handelsrelaties. Een aantal gepresenteerde modellen van vertrouwen beperkt zich tot de klant – leverancier relatie. Dit soort van relaties is te beperkt met het oog op de probleemstelling van dit onderzoek. Bij de data-uitwisseling van STIS worden commerciële, maar ook niet-commerciële data uitgewisseld.
- **Het type actor.**
  De actoren van het inter-organisationeel vertrouwen kunnen gevormd worden door personen, bedrijven of organisaties. Daarmee vallen o.a. de modellen die zich beperken tot interpersoneel vertrouwen af.

Op basis van deze selectiecriteria past het model van Ratnasingam het beste voor dit onderzoek.




**Figuur 2-1: Het conceptueel model voor vertrouwen volgens Ratnasingam.**

Op het moment dat Ratnasingam (2001) haar onderzoek startte, heeft ze een aantal cases uit de Australische auto-industrie onderzocht, waarbij EDI werd toegepast als mechanisme van data-uitwisseling tussen organisaties in de betreffende productieketen. Hierbij werden de uitgewisselde data gebruikt ten behoeve van de informatieverstrekking, maar tevens voor het aangaan van financiële verplichtingen. In de inleiding van haar onderzoek wijst ze erop, dat bij aanvang van haar onderzoek het begrip E-commerce nog niet bestond. Op dat moment

deed ze onderzoek naar het vertrouwen in EDI. Omwille van de groeiende aandacht voor het begrip E-commerce hanteert ze in haar onderzoek een zeer brede betekenis van het begrip E-commerce, waar commerciële en niet-commerciële activiteiten mee aangeduid worden. Data-uitwisseling volgens EDI is volgens haar onderzoek een deelverzameling van haar ruime begrip E-commerce.

Vervolgens heeft zij, voortbouwend op de bestaande modellen van haar voorgangers, een eigen model van vertrouwen ontwikkeld. Zij heeft dit model geschikt gemaakt voor het bepalen van de participatie aan E-commerce. Deze participatie aan E-commerce is voor haar de afhankelijke variabele welke beïnvloed wordt door de onafhankelijke variabelen relationeel en technologisch vertrouwen. Deze variabelen verhouden zich tot elkaar, zoals weergegeven in Figuur 2-1.

De door Ratnasingam gebruikte cases komen overeen met de omstandigheden waarin de data-uitwisseling van STIS zal plaatsvinden. Een aantal bedrijven binnen een branche gaan namelijk op een gestructureerde wijze data met elkaar uitwisselen. Een gebrek aan vertrouwen bedreigt het slagen van de data-uitwisseling.
Ratnasingam gebruikte haar model ten behoeve van het vertrouwen in E-commerce. Aangezien ze het begrip E-commerce in haar onderzoek ruim interpreteert, kan haar model tevens gelden voor STIS in de Nederlandse binnenvaartsector. Vanwege deze vergelijkbare situatie zal in dit onderzoek gebruik worden gemaakt van het model van Ratnasingam.

### *2.3.1 Relationeel vertrouwen*

Ratnasingam(2001) concludeert, na literatuurstudie over dit onderwerp, dat vertrouwen tussen partijen bestaat in 3 gradaties. De gradaties van vertrouwen bouwen op elkaar voort. De drie gradaties van vertrouwen zijn:

- Competence trust,
- Predictability trust en
- Goodwill trust

Het vertrouwen tussen deelnemende partijen ontwikkelt zich in een steeds 'hogere' vorm naarmate er meer positieve ervaringen worden opgedaan met de onderliggende vormen van vertrouwen. Hoe dit mechanisme functioneert wordt uitgelegd bij de verklaring van de gradaties van vertrouwen.

De basisvorm van vertrouwen tussen partijen heet 'Competence trust'. 'Competence trust' zal ontstaan bij een andere partij, zodra deze partij ervan overtuigd raakt dat vaardigheden, technische kennis en de bekwaamheid om de afgesproken E-commerce handelingen op een juiste wijze uit te voeren, aanwezig zijn bij de ene partij. Bij deze basisvorm van het vertrouwen is de ene partij overtuigd dat de competenties om de juiste handelingen te kunnen verrichten aanwezig zijn bij de andere partij.
Het genieten van deze vorm van vertrouwen is essentieel voor partijen, welke kwaliteitsproducten of –diensten naar andere partijen uitwisselen. Het vervaardigen van dit type van producten of diensten gebeurt veelal aan de hand van kwaliteitsborgende systematieken, welke ervan uit gaan, dat de elementaire technieken en vaardigheden beheerst worden. 'Competence trust' heeft uiteindelijk een economische grondslag. Het verwerven van dit soort van vertrouwen levert een directe besparing in kosten en tijd op. Het ontbreken van 'competence

trust' leidt tot extra kosten, voor b.v. het extra opleiden van personeel, of het opnieuw versturen van gecorrigeerde goederen of data.

'Predictability trust' ten aanzien van een andere partij ontstaat door consistent gedrag. Consistentie tussen wat een andere partij zegt en doet, maakt de partij betrouwbaar. De relatie met de andere partij ontwikkelt een hoog niveau van samenwerking en versterkt het vertrouwen in elkaar. 'Predictability trust' ontstaat door het herhaaldelijk tonen van 'competence trust'. Het maakt de andere partij voorspelbaar, en genereert daarmee een hoger niveau van vertrouwen in de andere partij. Echter, ervaringen met consistent negatieve gedragingen, kunnen leiden tot voorspelbaar wantrouwen. Er is in die situatie weer enige tijd nodig waarin consistentie in 'competence trust' wordt opgebouwd.

'Goodwill trust' zal ontstaan, indien de ene partij gelooft dat een andere partij eerlijk en betrouwbaar is. 'Goodwill trust' is de ultieme vorm van vertrouwen in een ander partij en komt voort uit 'competence' en 'predictability trust'. Bij deze hoogste vorm van vertrouwen ontwikkelt zich een emotionele band van zorg en bezorgdheid. Op dit niveau van vertrouwen ontstaat een grote loyaliteit ten opzichte van de andere partij.
(Ratnasingam, 2001)

### *2.3.2 Technologisch vertrouwen*

Naast het relationele vertrouwen (trust in trading partners), gaat Ratnasingam ervan uit, dat tevens een technologisch vertrouwen (trust & security based mechanisms) van invloed is op een participatie in E-commerce. Via de voordelen en de risico's van E-commerce maakt elke partij een afweging, in hoeverre ze kan of wil deelnemen aan data-uitwisseling activiteiten. Deze genoemde variabelen verhouden zich tot elkaar, zoals weergegeven in Figuur 2-1.

Het technologische vertrouwen is gebaseerd op ICT-technieken, welke zekerheid en garanties bieden voor het bedrijven van data-uitwisseling. Deze ICT-technieken zijn gericht op de beveiliging van de technische hulpmiddelen. Het technologische vertrouwen wordt geoperationaliseerd door de volgende variabelen:

- Vertrouwelijkheid: De bescherming van E-commerce transacties en berichtinhoud tegen ongeautoriseerd lezen, kopiëren of bekendmaken. Vertrouwelijkheid beproeft tevens de kwaliteit van de encryptiemechanismen en fire-walls in E-commerce systemen.
- Integriteit: De zekerheid dat E-commerce transacties niet worden gewijzigd of verwijderd. Integriteit toetst de kwaliteit van auditprocedures en de verrekeninstrumenten.
- Authenticiteit: De geloofwaardigheid of de echtheid. Authenticiteit beproeft de kwaliteit van de autorisatie mechanismen en de gehanteerde bevestigingsprocedures.
- Onweerlegbaarheid: Verzenders van E-commerce transacties kunnen niet ontkennen, dat ze berichten verzonden of ontvangen hebben. Onweerlegbaarheid toetst de kwaliteit van gehanteerde bevestigings- en uitsluitprocedures.
- Toegangscontrole: De bescherming van E-commerce transacties tegen zwakheden in de transmissie media en bescherming van de verzender tegen

interne fraude of manipulatie. Toegangscontrole beproeft de kwaliteit van de netwerk toegangscontrole en autorisatie mechanismen binnen E-commerce.
- Beschikbaarheid: De zekerheid, dat E-commerce transacties worden verzonden zonder onderbreking. Beschikbaarheid toetst het operationeel zijn van diensten en de beveiliging van het E-commerce netwerk.
- "Best practices": Deze " best practices" refereren naar het beleid, en de standaarden, welke het soepel functioneren van E-commerce operaties moet bewerkstelligen. "Best practices" beproeven de mate en de kwaliteit van management committent, vastgesteld beleid, gehanteerde procedures, risico analyses en gehanteerde management strategieën.

(Ratnasingam, 2001)

### *2.3.3 De voordelen van E-commerce*

De voordelen van E-commerce komen tot uiting in de kansen en winst (in brede zin van de betekenis), die partijen hebben gemaakt, door elektronische data-uitwisseling te adopteren. De onderliggende factoren zijn hierbij van toepassing:
- Economische voordelen: De voordelen, behaald uit directe besparingen in tijd en geld. Deze directe voordelen worden mede bepaald door de snelheid waarmee dit voordeel in tijd en geld wordt behaald. Een maat hiervoor is de terugverdientijd.
- Indirecte voordelen: Voorbeelden van indirecte voordelen zijn de kwaliteitsverbetering en de toegenomen nauwkeurigheid door het toepassen van elektronische data-uitwisseling en klanttevredenheid.
- Relatiegeoriënteerde voordelen: Dit betreft voordelen welke voortkomen uit een nauwere relatie met de handelspartner, zoals een open communicatie, data-uitwisseling en een hogere betrokkenheid.
- Strategische voordelen: Dit zijn voordelen voortkomende uit lange termijn investeringen en bewezen reputatie van handelsrelaties. Strategische voordelen worden geoperationaliseerd door imago, reputatie, en lange termijn investeringen in een handelsrelatie.

(Ratnasingam, 2001)

### *2.3.4 De risico's van E-commerce*

De risico's van E-commerce betreffen de potentiële zwakheden, de mogelijke drempels en verliezen, welke kunnen optreden de adoptie van E-commerce. De volgende onderliggende factoren zijn hierbij van toepassing:
- Technologisch falen: Het risico van het verkeerd inzetten van E-commerce technologie, virussen en het gebrek aan instrumenten voor de handhaving van vertrouwelijkheid, integriteit, geautoriseerde toegang of beschikbaarheid. Deze risico's komen tot uiting in de vorm van compatibiliteit, infrastructuur, complexiteit en onzekerheden in E-commerce systemen en activiteiten.
- Relationele risico's: Dit zijn risico's welke ontstaan door het gebrek aan kennis en training bij handelspartners, betreffende E-commerce. Dit risico uit zich in opportunistisch gedrag, conflicterende houdingen, slechte reputatie en een weerstand om van handelspartner te variëren.
- Algemene risico's: Deze risico's komen voort uit omgevingsfactoren, het ontbreken van toegepaste standaards en een gebrek aan controle. Deze risico's worden geoperationaliseerd door standaardisatie en beveiligingsdiensten.

(Ratnasingam, 2001)

### *2.3.5 De participatie aan E-commerce*

De participatie in E-commerce is de mate waarin een partij deelneemt in de adoptie, integratie en het gebruik van elektronische data-uitwisseling. De factoren, welke bepalend zijn voor de participatie in E-commerce, zien er als volgt uit:

- De omvang van de E-commerce prestatie; deze prestatie wordt gemeten in volume, omzet en typen van zakelijke transacties.
- De ontwikkeling van de vertrouwensrelatie tussen de handelspartners; deze variabele wordt geoperationaliseerd door samenwerking, open communicatie, betrokkenheid, reputatie en lange termijn investeringen in relaties.

(Ratnasingam, 2001)

## 2.4 De toepasbaarheid van het conceptuele model voor STIS

### *2.4.1 Inleiding*

In deze paragraaf vindt de confrontatie plaats tussen het geselecteerde model uit de vorige paragraaf en de specifieke problematieken, waarin het model binnen STIS zal moeten voorzien. Uit deze confrontatie zal blijken hoe goed het model toepasbaar is op de problematiek van STIS. De toepasbaarheid van het model wordt getoetst aan de gevoeligheden in de data-uitwisseling van STIS.
In paragraaf 2.4.2 worden de gevoeligheden in de data-uitwisseling van STIS omschreven.
In paragraaf 2.4.3 wordt de confrontatie uitgevoerd van deze gevoeligheden met het model van Ratnasingam, welke resulteert in een conceptueel model voor de beschrijving van het vertrouwen van STIS.

### *2.4.2 De gevoeligheden bij de data-uitwisseling van STIS*

In de inleiding (paragraaf 1.1) zijn de vier onderstaande soorten van data-uitwisseling genoemd, waarbij naar verwachting een gebrek aan vertrouwen kan ontstaan. De volgende gevoeligheden worden verwacht (Kuiters-Goederen, 2002):

- Privacygevoelige gegevens;
- Bedrijfsgevoelige gegevens;
- Kwaliteit van nautische gegevens;
- De status van de elektronische transactie.

**Privacygevoelige gegevens**

Van de ongeveer 5000 Nederlandse binnenvaartschepen is 97% in het bezit van particuliere binnenvaartondernemingen (Vries, 2000). Dit zijn voornamelijk bedrijven met één schip in de vaart. De laatste 10 jaar worden ladingen in varende schepen geregistreerd door middel van landelijk dekkende informatiesystemen. Deze registratie stimuleert de veiligheid en de vlotheid van het verkeer op de binnenwateren. In deze informatiesystemen worden gegevens betreffende schip, lading, reis en opvarenden geregistreerd. Een deel van deze registraties betreft de identiteit van de eigenaar van het schip, welke zich in de meeste gevallen op het betreffende schip bevindt. Deze gegevens hebben betrekking op de privacy van de schipper. De identificatie van een vaartuig vindt plaats door middel van de officiële scheepsnaam en een lijst waarin de bijbehorende eigenaar is terug te vinden. Deze lijsten met officiële scheepsnamen en bijbehorende eigenaren zijn openbaar. In de informatiesystemen, welke binnen

de binnenvaart worden toegepast, kunnen de handelingen en gedragingen van dit vaartuig (en dus ook de eigenaar), gevolgd worden. Volgens de Wet Bescherming Persoonsgegevens (WBP) is hier sprake van een persoonsregistratie. Met het uitvoeren van de scheepvaartregistratie worden dus persoonsgerelateerde gegevens vastgelegd.

Het uitvoeren van deze registraties ligt nog steeds erg gevoelig in de binnenvaartsector. De invoering van een privacyreglement in het kader van de Wet Persoonsregistratie (ongeveer 5 jaar geleden) heeft onder de particuliere binnenvaartondernemingen een groot vertrouwen opgeleverd. Met de implementatie van STIS worden persoonlijke gegevens door een groter aantal partijen on-line gekoppeld met andere bestanden. Het bouwen aan het vertrouwen door de juiste behandeling van de privacygevoelige gegevens zal opnieuw moeten plaatsvinden.

Zodra blijkt dat deze persoonlijke gegevens worden uitgewisseld ten behoeve van andere doeleinden, zal wantrouwen ontstaan bij de individuele schipper. Het gebruik van deze gegevens voor andere doeleinden zal op den duur de primaire registraties (waarvoor de schipper ze oorspronkelijk beschikbaar had gesteld) schaden. De schippers zullen het nalaten deze gegevens te laten registreren. Dit zal vervolgens weer een bedreiging kunnen worden voor de veiligheid en de vlotheid op de vaarwegen en de vaarwegknooppunten.
Voorbeelden van misbruik van privacygevoelige gegevens zijn:

- de passagetijden bij sluizen of bruggen, welke de schippers aan de vaarwegbeheerders verstrekt, kunnen door handhavers worden gebruikt voor de controle op de vaar- en rusttijden wetgeving;
- het registreren van het ligplaatsengebruik in havens door de vaarwegbeheerders, waardoor de havenbedrijven op basis van deze registraties de havengelden kunnen innen.

**Bedrijfsgevoelige gegevens**
Bedrijfsgevoelige gegevens bevatten informatie over het operationeel of strategisch handelen van een commerciële onderneming, als deelnemer aan STIS. Deze informatie kan, in handen van een partij die hetzelfde marktsegment benadert, economische schade veroorzaken. Voorbeelden van misbruik met betrekking tot dit soort gegevens zijn:

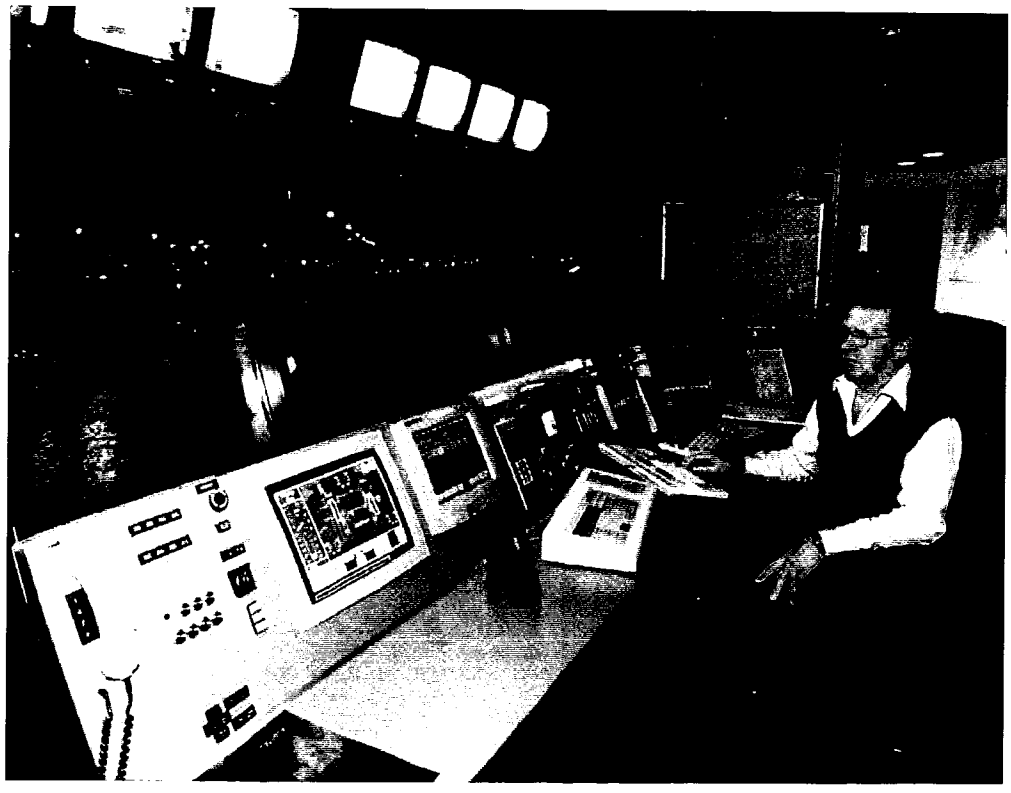
- de concurrent kan informatie verkrijgen, waardoor inzicht ontstaat in de strategie van een onderneming; de concurrentiestrategie van de andere onderneming kan op basis van deze informatie bepaald worden.
- het relatienetwerk van een binnenvaartonderneming kan schade oplopen, doordat een concurrent een zelfde relatie voor zich kan proberen te winnen.
- een aantal terminalbeheerders is tevens eigenaar van een aantal binnenvaartschepen. Deze terminalbeheerders krijgen informatie betreffende alle schepen die lading bij hun terminal komen laden of lossen. Ook van de binnenvaartschepen die niet onder hun vlag varen. Door de dubbele rol van deze terminalbeheerders kunnen zij wel in het bezit komen van bedrijfsgevoelige informatie.

Operationeel gevoelig zijn gegevens, die inzicht verschaffen betreffende het handelen van een partij rondom één transport. Als voorbeeld geldt: welk type lading op welk moment van welke herkomst naar welke bestemming vervoerd moet worden.
Strategisch gevoelig zijn gegevens, die het bedrijfsmatig handelen van een partij beschrijven, gedurende een bepaalde periode. Hieruit kan een inzicht ontstaan

met betrekking tot bedrijfsresultaten en strategieën van een onderneming. Deze informatie is van belang voor concurrenten in dezelfde markt.

In de binnenvaartsector treedt schaalvergroting op; steeds grotere schepen worden gebouwd om grotere partijen in een transport te kunnen verplaatsen. De investeringen van de particuliere ondernemer worden hierdoor groter. Het op een juiste wijze omgaan met bedrijfsgevoelige gegevens is erg belangrijk voor deze kwetsbare groep uit de binnenvaartsector.

**Kwaliteit van de nautische gegevens**
Een onderdeel van STIS is het elektronisch verstrekken van nautische gegevens. Dit type van gegevens wordt door de schippers op dit moment nog via conventionele communicatiemedia vergaard (boekwerken, teletekst, via het marifoonkanaal opvragen bij beheerders en soms Internet). De verstrekkers van deze conventionele informatie nemen geen aansprakelijkheid voor de kwaliteit van de nautische gegevens.
De traditioneel gebruikte rivierkaarten hebben een update-interval van 3 jaar. De schippers kenden dit fenomeen, zodat ze steeds alert moesten blijven op gewijzigde situaties op de vaarweg, in afwijking van de laatste versie rivierkaarten.



**Figuur 2-2: De data-uitwisseling vanaf de sluis.**

Bepaalde soorten van on-line gegevens worden gepresenteerd door applicaties van derden (b.v. vaarwegkaarten met de presentatie van een beschikbare vaargeul). Deze on-line presentatiewijze suggereert een grote nauwkeurigheid. In het geval van dynamische verkeerstekens (betonning, bebording) aan of op vaarwegen is er telkens sprake van een vertraging in de update van de nieuwe

gegevens. De rivierbeheerder zal in veel gevallen eerst de bebakening aanpassen en vervolgens de on-line data gaan wijzigen. Zelfs met de verstrekking van on-line gegevens zal de schipper alert moeten blijven op lokale afwijkingen ten opzichte van de gepresenteerde data.
Door het on-line beschikbaar stellen van data en het frequenter verversen van deze data suggereert de verstrekker een grotere mate van nauwkeurigheid. Daardoor zal de verstrekker van deze data een grotere verantwoordelijkheid krijgen voor de juistheid van de beschikbaar gestelde gegevens.
In geval van schade of gevaar voor de (externe) veiligheid, zal de vraag van de aansprakelijkheid worden gesteld. Door de gesuggereerde nauwkeurigheid van de verstrekte data kan de vaarweggebruiker wijzen op een onjuistheid van gepresenteerde data. De beheerder wijst ook in de toekomst de aansprakelijkheid hiervoor af.

De kwaliteit van de (nautische) gegevens is doorgaans van toepassing op uitwisseling van gegevens van overheden naar commerciële ondernemingen. Indien hierbij onjuiste of onvolledige data wordt verstrekt, kunnen de overheden als bron van informatie aansprakelijk worden gesteld. Bij een gebrekkige doorgifte van nautische gegevens van vaarwegbeheerder (overheid) naar schipper (bedrijf) kan voor de schipper leiden tot forse schade.

**De status van de elektronische transactie**
Na implementatie van STIS zullen een groot aantal partijen uit de binnenvaartsector een stelsel van afspraken overeenkomen, zodat een gestandaardiseerde elektronische berichtenuitwisseling tussen informatiesystemen van de deelnemende partijen mogelijk wordt. Deze vorm van berichtuitwisseling is te typeren als EDI, zoals in paragraaf 1.3.3 is beargumenteerd.

De invoering van EDI-toepassingen is niet uitsluitend een technische aangelegenheid. De veranderde manier van samenwerken en de vervanging van papieren documenten door elektronische berichten vragen om nieuwe spelregels. Een aantal juridische aspecten (Vlist e.a., 1994, p. 167) verdient hierbij speciale aandacht. De volgende juridische aspecten zijn namelijk in de huidige wetgeving niet eenduidig omschreven:

- De geldige totstandkoming van een overeenkomst;
- De schriftelijke handelsdocumenten, waarin de eigendom van zaken of een vordering is belichaamd;
- De bewijslast in geval van een meningsverschil;
- Het vaststellen van de identiteit en de bevoegdheid van de afzender;
- De aansprakelijkheid voor fouten in de berichtgeving;
- De bewaring van EDI-berichten.

Deze onduidelijkheid in de wetgeving kan een gebrek aan vertrouwen tussen deelnemende partijen aan STIS gaan opleveren. De status van de elektronische transactie levert bijvoorbeeld een onzekere juridische status op in het geval van:

- een uitwisseling van gegevens tussen bedrijven, welke van invloed kunnen zijn op commerciële overeenkomsten. Indien een verlader een verkeerd gegeven verstrekt, waardoor de schipper uiteindelijk de opdracht niet kan uitvoeren conform de intentie van de verlader, zullen deze twee partijen elkaar aanwijzen als de veroorzaker;
- de meldplicht van bepaalde typen schepen en transporten. Voor het verkeersmanagement is het van belang, dat een melding ook daadwerkelijk

aankomt. Wat gebeurt er indien de melding niet (tijdig) of niet op de juiste plek wordt bezorgd?

De onzekerheid over de status van elektronische transactie is een punt van zorg voor de potentiële deelnemers aan STIS.

### *2.4.3 Confrontatie van Ratnasingam met STIS*

Het model van Ratnasingam uit Figuur 2-1 wordt in deze paragraaf geconfronteerd met het wantrouwen dat in het project STIS dreigt te ontstaan bij de partijen van STIS. Deze confrontatie zal uiteindelijk Figuur 2-3 opleveren, 'Het conceptuele model van het vertrouwen in de elektronische data-uitwisseling van STIS.'

| Variabele model Ratnasingam | Variabele conceptueel model STIS |
|---|---|
| Relationeel vertrouwen | Relationeel vertrouwen |
| Technologisch vertrouwen | Technologisch vertrouwen |
| - | Juridisch vertrouwen |
| De voordelen van E-commerce | - |
| De risico's van E-commerce | De risico's van elektronische data-uitwisseling |
| De participatie aan E-commerce | De participatie aan STIS |

**Tabel 2-1: Conversie van variabelen van het model van Ratnasingam naar STIS**

Voor de diverse variabelen uit het model van Ratnasingam wordt nagegaan, of, en op welke wijze ze een rol van betekenis spelen bij de data-uitwisseling van STIS. Het resultaat van de confrontatie levert Tabel 2-1 op.

Het gebrek aan vertrouwen in de data-uitwisseling van STIS wordt geoperationaliseerd door de vier vormen van gevoeligheden (zoals omschreven in paragraaf 2.4.2) bij de data-uitwisseling van STIS. Volgens de operationalisatie van de variabele 'De voordelen van E-commerce' in paragraaf 2.3.3, levert het gebrek aan vertrouwen in STIS geen enkel voordeel op voor de data-uitwisseling van STIS. Er zijn uitsluitend nadelen te verwachten. Daarom is de variabele 'De voordelen van elektronische data-uitwisseling' niet relevant voor de probleemstelling van dit onderzoek.

Het verschijnen van de variabele 'Juridisch vertrouwen' wordt uitgelegd bij de beschrijving van de variabele 'De risico's van elektronische data-uitwisseling'.

De volgende alinea's bespreken de variabelen van het conceptueel model voor STIS, zoals deze volgens Tabel 2-1 van toepassing zullen zijn.

**De participatie aan STIS**

De afhankelijke variabele van het gebruikte model (De participatie aan STIS) past op de doelstelling van het STIS-project: een succesvolle implementatie van STIS. Een succesvollere implementatie van STIS wordt gerealiseerd indien meer beoogde deelnemers gaan participeren in STIS.

Volgens het conceptuele model van STIS heeft 'De participatie aan STIS' uitsluitend een relatie met 'De risico's van elektronische data-uitwisseling'. De vier gevoeligheden bij de data-uitwisseling leveren immers uitsluitend risico's op voor de data-uitwisseling van STIS.

Het reduceren van 'De risico's van elektronische data-uitwisseling' zal resulteren in een vergroting van 'De participatie aan STIS'. Voor een optimaal

resultaat van het project STIS is het van belang 'De risico's van elektronische data-uitwisseling' zo laag mogelijk te houden.

**De risico's van elektronische data-uitwisseling**
In paragraaf 2.3.4 zijn de volgende variabelen onderkend voor de risico's van elektronische data-uitwisseling:
- technologisch falen;
- relationele risico's;
- algemene risico's.

Het technologisch falen is voor alle soorten van gevoeligheden van de data-uitwisseling een risico. Elk van de gevoeligheden van data-uitwisseling is dus afhankelijk van het juist functioneren van technologie. Voor deze elektronische data-uitwisseling is het juist functioneren van beveiligingsmaatregelen cruciaal. Voor de gebruikers van de deelnemende partijen is het disfunctioneren van de ICT snel waarneembaar.
Bijvoorbeeld netwerkverbindingen worden niet of verkeerd opgebouwd, afscherming van data vindt niet plaats, ontvangstbevestigingen van elektronisch gesloten overeenkomsten blijven uit, enz. Enerzijds is het openbaar maken van gevoelige informatie zeer onwenselijk, maar anderzijds is het stoppen van de data-uitwisseling evenmin wenselijk voor de deelnemers aan STIS. De technologie zal op een dusdanige zorgvuldige wijze ontworpen moeten worden, dat een technologisch falen niet kan leiden tot een gebrekkige beschikbaarheid.

De relationele risico's kunnen ontstaan, indien de ene partij geen consistentie kan bereiken in het handelen. Bij alle typen van gevoeligheden is dit consistent gedrag van de deelnemers aan STIS van groot belang. Dit consistent gedrag kan ontbreken vanwege onkunde of onwil om het gewenste handelen te vertonen.

De algemene risico's kunnen ontstaan bij het ontbreken van standaardisatie. Bij alle typen van gevoeligheden is de wettelijke verankering (standaardisatie) nogal gebrekkig. De gebruikers zijn onzeker in het maken van de keuzes, aangezien ze geen houvast hebben aan een algemeen gebruikte standaard (wettelijk kader) welke voldoende zekerheid biedt.

**Relationeel, technologisch en juridisch vertrouwen**
De onafhankelijke variabelen van het conceptuele model van STIS bestaan uit relationeel technologisch en juridisch vertrouwen. In de confrontatie van het model met STIS, wordt afgewogen welk van deze onafhankelijke variabelen een oplossing kan bieden voor de gevoeligheden van STIS. De genoemde gevoeligheden bij de data-uitwisseling van STIS worden vervolgens vergeleken met deze onafhankelijke variabelen.

Bij relationeel vertrouwen speelt het menselijk handelen binnen de betreffende organisaties een rol van betekenis. Het menselijk handelen dient daarbij afgestemd te zijn op de gemaakte afspraken tussen de deelnemende organisaties van STIS, en de consistentie in dit gedrag. Het consistent menselijk handelen is van toepassing op alle soorten van gevoeligheden.
Deze specifieke vorm van vertrouwen kan voor dit onderzoek gedefinieerd worden met behulp van de gekozen algemene definitie van vertrouwen. Relationeel vertrouwen is:

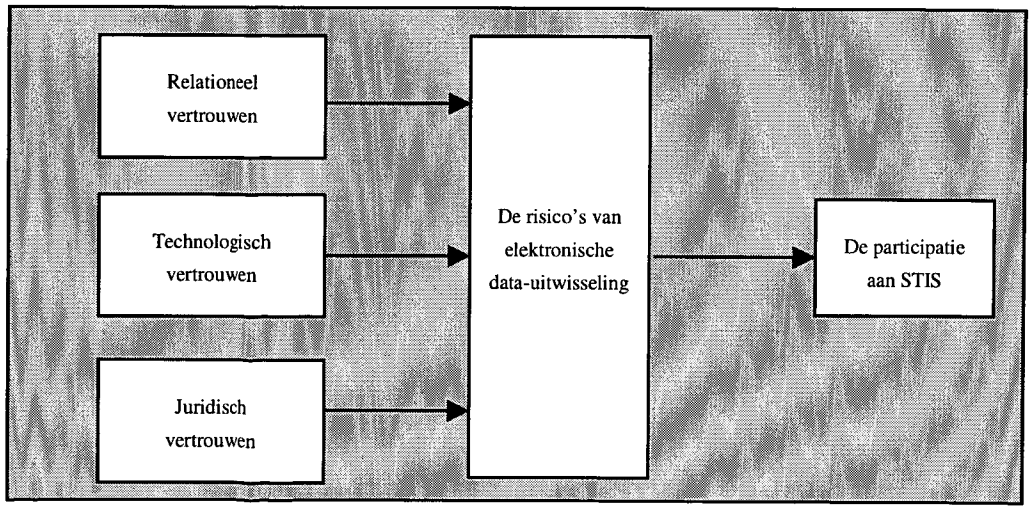
> *"De overtuiging van de ene partij, dat de andere partij in de uitwisselingsrelatie, haar relationele kwetsbaarheid niet zal uitbuiten."*

Het vergroten van het relationeel vertrouwen zal dus plaatsvinden door het reduceren van de relationele kwetsbaarheden. Deze relationele kwetsbaarheden komen overeen met de 'relationele risico's' zoals deze door Ratnasingam zijn gedefinieerd.

Zoals in de inleiding van dit rapport aangeduid, is STIS geen architectuur voor een nieuw informatiesysteem. De gepresenteerde functionaliteit van STIS zal toch een sterke technologische component krijgen, doordat er nieuwe technologische componenten geïntroduceerd gaan worden, welke de efficiënte data-uitwisseling tussen de bestaande informatiesystemen gaan realiseren.
Onder de gebruikers bestaat er een scepsis bij de introductie van nieuwe informatieverwerkende technologie. De ervaring van ICT-gebruikers, dat nieuwe informatiesystemen zelden foutloos functioneren vanaf de eerste ingebruikname, voedt dit gebrek aan technologisch vertrouwen sterk. Het aspect technologisch vertrouwen speelt een belangrijke rol voor alle soorten van gevoeligheden bij data-uitwisseling van STIS. Zoals hierboven bij de risicofactor "technologisch falen" reeds aangeduid, zal een stabiel en betrouwbaar ontworpen uitwisselingsmechanisme, aangevuld met gedegen beveiligingstechnieken, een belangrijke pijler zijn voor het vertrouwen in de data-uitwisseling van STIS.
Ook deze specifieke vorm van vertrouwen wordt voor dit onderzoek gedefinieerd met behulp van de gekozen algemene definitie van vertrouwen. Technologisch vertrouwen is:

> *"De overtuiging van de ene partij, dat de andere partij in de uitwisselingsrelatie, haar technologische kwetsbaarheid niet zal uitbuiten."*

Het vergroten van het technologisch vertrouwen zal dus plaatsvinden door het reduceren van de technologische kwetsbaarheden. Deze technologische kwetsbaarheden komen overeen met het 'technologische falen' zoals dit door Ratnasingam is gedefinieerd.




**Figuur 2-3: Het conceptuele model van het vertrouwen in de elektronische data-uitwisseling van STIS.**

Naast de twee onafhankelijke variabelen uit het model van Ratnasingam (relationeel en technologisch vertrouwen) is er voor STIS nog een derde component

van invloed op "De participatie aan STIS". Volgens Esch (Esch-1, 1999) en Vlist (Vlist et. al., 1994) is het onvoldoende afgestemd zijn van de huidige Nederlandse wetgeving een belangrijke oorzaak van het gebrek aan vertrouwen in elektronische data-uitwisseling ten behoeve van transacties. Bij de ontwikkeling van de elektronische data-uitwisseling was het bestaande juridische kader vaak ontoereikend. Ook bij de overige gevoeligheden van de data-uitwisseling ontbreekt een sluitend juridisch kader.
Het model van Ratnasingam voorziet niet in een onafhankelijke variabele, welke een indicatie was voor het vertrouwen in het juridisch kader voor de data-uitwisseling. Door het ontbreken van een sluitend juridisch kader bestaat behoefte aan een aanvullende onafhankelijke variabele binnen het conceptuele model van STIS. Het model uit Figuur 2-3 bevat daarom aanvullend de onafhankelijke variabele "Juridisch vertrouwen".
Ook deze specifieke vorm van vertrouwen wordt voor dit onderzoek gedefinieerd met behulp van de gekozen algemene definitie van vertrouwen. Juridisch vertrouwen is:

> *"De overtuiging van de ene partij, dat de andere partij in de uitwisselingsrelatie, haar juridische kwetsbaarheid niet zal uitbuiten."*

Het vergroten van het juridisch vertrouwen zal dus plaatsvinden door het reduceren van de juridische kwetsbaarheden. Deze juridische kwetsbaarheden vormen een onderdeel van de 'algemene risico's' zoals deze door Ratnasingam zijn gedefinieerd.
Een voorbeeld van juridische kwetsbaarheid is het afsluiten van een contract via elektronische data-uitwisseling, terwijl de wetgeving in deze niet eenduidig is. Deze partij is kwetsbaar op juridisch vlak.

## 2.5 Conclusie

Het toe te passen conceptueel model voor de data-uitwisseling van STIS is weergegeven in Figuur 2-3. De onafhankelijke variabelen 'Relationeel vertrouwen', 'Technisch vertrouwen' en 'Juridisch vertrouwen' zijn van invloed op de afhankelijke variabele 'De participatie aan STIS'. Voor elk van de drie onafhankelijke variabelen geldt, dat ze de afhankelijke variabele positief beïnvloeden, indien de betreffende onafhankelijke variabele positief van aard is.

Uit paragraaf 2.4.3 is gebleken, dat de onafhankelijke variabelen van het model van STIS allen direct van invloed zijn op elk van de gevoeligheden van STIS. In het volgende hoofdstuk wordt daarom gezocht naar maatregelen, die een of meerdere onafhankelijke variabelen van het STIS-model op een positieve wijze zullen beïnvloeden.

# 3 De maatregelen die het vertrouwen vergroten

In hoofdstuk 2 is het conceptuele model gepresenteerd, waarmee de participatie aan STIS beïnvloed kan worden. In dit hoofdstuk worden maatregelen aangereikt, welke de onafhankelijke variabelen uit het conceptuele model ('Relationeel vertrouwen', het 'Technologisch vertrouwen' en het 'Juridisch vertrouwen') van Figuur 2-3 op een positieve wijze beïnvloeden. Per maatregel zal worden aangegeven welk soort van vertrouwen wordt beïnvloed.

Vanuit literatuur wordt een breed scala van maatregelen genoemd, welke het vertrouwen in de data-uitwisseling tussen computersystemen kunnen vergroten. In de volgende paragrafen worden deze maatregelen gebundeld in een beperkt aantal categorieën. Voor elk van de categorieën wordt aangegeven welke van de literatuurverwijzingen bepalend zijn geweest voor het selecteren van de gepresenteerde maatregelen.

- Informatiebeveiliging
  Overbeek, 2000; Esch-1, 1999; Esch-2, 2002; Tanenbaum, 1999.
- Opleiding en training
  Ratnasingam, 2001.
- Interchange Agreement
  Esch-1, 1999; Esch-2, 2002; Franken et. al., 2001; Klaauw-1, 1995; Klaauw-2, 2002; Stuurman en Wijnands, 1998.
- Trusted Third Party
  Duthler, 1998; Esch-1, 1999; Franken et. al., 2001.
- Aanpassingswet Elektronische Handel
  Gijrath & Kolthek, 2002; Franken et. al., 2001.

Uit deze literatuur worden maatregelen voorgedragen van technische, organisatorische en juridische aard, welke voor STIS van invloed kunnen zijn op de onafhankelijke variabelen van het STIS-model.

In dit hoofdstuk worden de mogelijke maatregelen voor STIS geaccentueerd door een verticale streep in de kantlijn, met daarbij een nummering per maatregel. Op die manier zijn de aanbevelingen uit dit rapport eenvoudig te herkennen en te benoemen. De wijze van implementatie en de prioritering van deze maatregelen in STIS wordt in hoofdstuk 4 uitgewerkt.

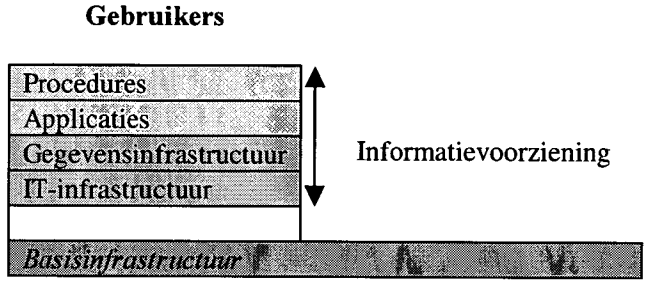
## 3.1 De informatiebeveiliging

### *3.1.1 Inleiding*

Het technologisch vertrouwen wordt volgens de onafhankelijke variabele van het conceptuele model beïnvloed door de volgende aspecten: vertrouwelijkheid, integriteit, authenticiteit, onweerlegbaarheid, toegangscontrole, beschikbaarheid en de toepassing van "Best practices". Door middel van informatiebeveiliging worden al deze aspecten positief beïnvloed. Hierdoor zal vervolgens het technologisch vertrouwen in STIS vergroot worden (Ratnasingam, 2001).
Door de inzet van informatiebeveiliging zal tevens het relationeel vertrouwen worden beïnvloed. Het relationeel vertrouwen wordt volgens de onafhankelijke variabele van het conceptuele model beïnvloed via de volgende aspecten: beheersing van de elementaire technieken en vaardigheden, consistentie in handelen en loyaliteit (Ratnasingam, 2001). De informatiebeveiliging beïnvloedt

deze aspecten op positieve wijze. Hierdoor zal ook het relationeel vertrouwen in STIS vergroot worden.

Informatiebeveiliging is een verzamelnaam voor de processen, die ingericht worden om de betrouwbaarheid van de informatiesystemen en de daarin opgeslagen gegevens te beschermen tegen al dan niet opzettelijk onheil (Overbeek, 2000).




**Figuur 3-1: Componenten van de informatievoorziening**

Het model van Overbeek (Figuur 3-1) wordt als basis genomen voor het bepalen van de maatregelen voor STIS op het vlak van de informatiebeveiliging. Het model beschrijft de componenten van de informatie voorziening. De beveiligingsmaatregelen strekken zich uit over de procedures, de applicaties, de gegevensinfrastructuur, de IT-infrastructuur en de basisinfrastructuur.

De mogelijke beveiligingsmaatregelen kunnen fysiek, logisch of organisatorisch van aard zijn (Figuur 3-2).

- De fysieke maatregelen zijn toepasbaar op de apparatuurdelen van de infrastructuren. Een deel hiervan richt zich op de basisinfrastructuur, en een ander deel richt zich op de IT-infrastructuur. De maatregelen zijn gebaseerd op apparatuur of andere materiële zaken. Voorbeelden hiervan zijn: noodstroomvoorzieningen, brandblusinstallaties, deursloten en andere bouwkundige voorzieningen. De mogelijke toe te passen maatregelen worden in paragraaf 3.1.2 genoemd.
- De logische maatregelen zijn toepasbaar op programmatuur (applicaties) en op gegevensverzamelingen (gegevensinfrastructuur). Voorbeelden hiervan zijn: Log-in en wachtwoordauthenticatie in besturingssystemen, encryptieprogrammatuur voor het vercijferen van vertrouwelijke gegevens, digitale handtekeningen in elektronische berichten. De mogelijke toe te passen maatregelen worden in paragraaf 3.1.3 genoemd.
- De organisatorische maatregelen worden toegepast op de procedures binnen de betreffende organisaties en op het gedrag en de bewustwording van de gebruikers van de applicaties en de data. Voorbeelden hiervan zijn: Het inrichten van een PKI-infrastructuur en het hanteren van certificatie. De mogelijke toe te passen maatregelen worden in paragraaf 3.1.4 genoemd.

### *3.1.2 Fysieke maatregelen*

Volgens Figuur 3-2 worden logische maatregelen voornamelijk toegepast op het niveau van de basis- en de IT-infrastructuur. Voor deze infrastructuur voorziet Overbeek de volgende bedreigingen:

**IT-infrastructuur**

Apparatuur:

- Externe oorzaken (brand, bliksem, water, storm, verkeer, aardbeving)

- Storingen in apparatuur van de IT-infrastructuur;
- Onopzettelijk foutief handelen;
- Opzettelijk foutief handelen (inbraak, diefstal).

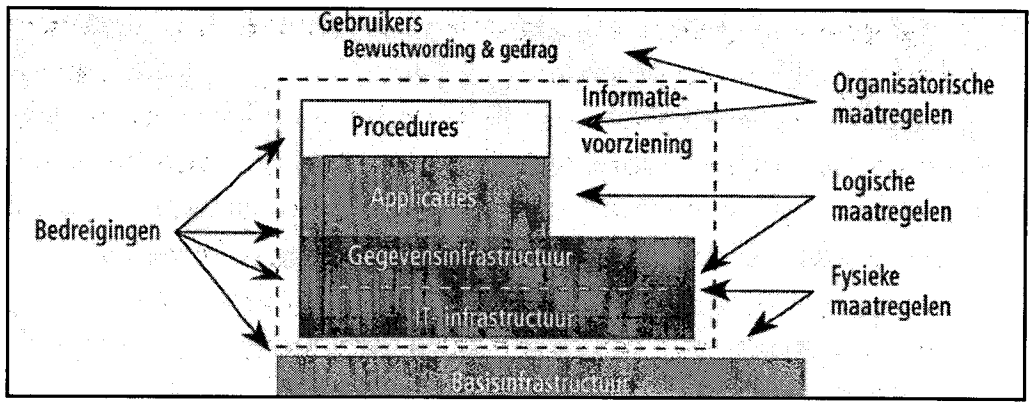
Software:

- Storingen in de programmatuur van de IT-infrastructuur;
- Onopzettelijk foutief handelen;
- Opzettelijk foutief handelen (virussen, hackers, gebruik illegale programmatuur).

**Basisinfrastructuur**

- Elektro;
- Telecom;
- Airco;
- Water;
- Gebouw.

**Bron: Overbeek, 2000**




**Figuur 3-2: De beveiligingsmaatregelen en hun werkgebied.**

Tegen de hierboven genoemde bedreigingen zijn een aantal mogelijke preventieve maatregelen mogelijk (Overbeek, 2000). In onderstaande opsomming worden de fysieke maatregelen toegelicht, welke voor STIS in aanmerking kunnen komen.

**Back-up maatregelen**

Maatregel 1.

Deze maatregelen zijn gebaseerd op het maken van reservekopieën. Back-up maatregelen wordt gebruikt voor het herstellen van bestanden van applicaties of gegevensverzamelingen die in ongerede zijn geraakt.

Bij het maken van een back-up voor STIS zijn de volgende aspecten relevant:

- De frequentie van het genereren van een back-up moet worden afgestemd op de verversing van de bestanden.
- De plaats waar de back-up bestanden worden opgeslagen. Er bestaan verschillende soorten van bedreigingen waarbij naast het originele bestand tevens de back-up bestanden in ongerede kunnen raken. Dit dient afgewogen worden tegenover de af te leggen afstand naar de opslag van back-upbestanden.

(Overbeek, 2000)

**Uitwijkfaciliteiten voorzien**

Maatregel 2. Uitwijken is het terugvallen op een reservefaciliteit, als de eigen faciliteit niet meer beschikbaar is. De mogelijkheid om uit te wijken wordt gebruikt om continuïteit zeker te kunnen stellen na het optreden van een calamiteit. Bij het uitwijken wordt een andere IT-infrastructuur stand-by in geval van een calamiteit (Overbeek, 2000).

### *3.1.3 Logische maatregelen*

Volgens Figuur 3-2 worden logische maatregelen voornamelijk toegepast op applicatieniveau en ten behoeve van de gegevensinfrastructuur. Voor applicaties en gegevensinfrastructuur voorziet Overbeek de volgende bedreigingen:

- Storingen in applicaties en gegevensinfrastructuur;
- Onopzettelijk foutief handelen;
- Opzettelijk foutief handelen.

Tegen de hierboven genoemde bedreigingen zijn een aantal mogelijke preventieve maatregelen mogelijk (Overbeek, 2000). In onderstaande opsomming worden de fysieke maatregelen toegelicht, welke voor STIS in aanmerking kunnen komen.

**Toegangsbeheersing**

De bescherming tegen menselijke bedreiging is volgens Overbeek het meest effectief door de beheersing van de onbevoegde toegang tot de informatiesystemen en gegevens (Overbeek, 2000).

Maatregel 3. Toegangsbeheersing beoogt ervoor te zorgen dat personen of systemen wel de beschikking hebben over de gegevens en functies die ze nodig hebben, maar niet over de gegevens en functies die ze niet nodig hebben, of waarvan het vanwege het vertrouwelijke karakter niet wenselijk is dat ze er toegang toe hebben. (Overbeek, 2000)

De logische maatregelen kunnen betrekking hebben op het afsluiten van (computer-)ruimten, tot het afschermen van computersystemen en applicaties met een wachtwoordsysteem.

Toegangsbeheersing omvat het:

- Specificeren van de toegang. In toegangsregels wordt gespecificeerd welke personen welke bevoegdheden hebben met betrekking tot welke bestanden.
- Verlenen van de toegang. Op basis van de gedefinieerde toegangsregels kan al dan niet toegang verleend worden aan personen die daar om verzoeken. Hierbij worden de stappen doorlopen van identificatie (bepaling identiteit), authenticatie (verifiëren van de geclaimde identiteit) en autorisatie (toekennen van rechten).
- Bewaken van de toegang. Het bewaken van toegang omvat het detecteren van inbreuken op de toegangsregels en het registreren daarvan.

**Netwerkbeveiliging**

De maatregelen voor het realiseren van netwerkbeveiliging zijn deels fysiek en deels logisch van aard, indien het OSI-model voor netwerken gehanteerd wordt. De mogelijkheden tot fysieke beveiliging wordt bepaald door het type transmissiemedium dat gekozen is. Geleide media (zoals UTP, coax of glasvezel) zijn goed af te schermen, terwijl voor ongeleide media (zoals radio-infrarood- of microgolven) dit haast niet mogelijk is. De signalen kunnen door elke ontvanger binnen het bereik worden opgevangen.

Maatregel 4. De netwerkbeveiliging van datatransmissie via ongeleide media (toegepast bij mobiele communicatiemiddelen) wordt volledig gerealiseerd op basis van

logische maatregelen. Een groot deel van de data-uitwisseling binnen STIS vindt mobiel plaats. Daarom zal de netwerkbeveiliging veel aandacht vergen.
Voor de netwerkbeveiliging van geleide media is het van groot belang, dat de toegangsbeheersing tot netwerkknooppunten van hoge kwaliteit is. De routers, de hubs, routers, switches en de telefooncentrales zijn de zwakke schakels in de geleide netwerktechniek.

Veel netwerken zijn tegenwoordig gebaseerd op het Internet Protocol (IP). IP heeft een aantal voordelen ten opzichte van de andere bestaande protocollen: het 'open' karakter, de robuustheid, de efficiëntie en het wereldwijde adresseringsschema. De beveiliging van netwerken richt zich op de koppeling van de interne (bedrijfsnetwerken) met de externe netwerken. De relevante technieken voor toepassing binnen STIS zijn (Tanenbaum, 1999):

- Packet-filter firewalls: Deze firewall is een normale router (checkt de IP-adressering) waarop extra functies voorhanden zijn. Dit type firewall grijpt in op de netwerklaag (OSI).
- Proxy firewalls: Deze firewall checkt op applicatieniveau of een pakket toegelaten mag worden tot het te beveiligen netwerk.

Aanvullende voorzieningen voor firewalls, die het beveiligingsniveau verhogen, kunnen zijn (Overbeek, 2000):

- Logging en monitoring. Hiermee wordt een poging tot onbevoegd handelen direct gesignaleerd en gemeld.
- Tunneltechnieken. Gekoppelde interne netwerken zetten een onderlinge verbinding op via het 'onveilige' Internet. Door middel van vercijfering ('encrypted tunneling') wordt deze verbinding beveiligd.

**Antivirus-maatregelen**

Van de vele soorten kwaadaardige programma's zijn computervirussen de bekendste. Al deze kwaadaardig programma's hebben de opzet ongewenste activiteiten uit te voeren binnen de hardware, de besturingssystemen, de applicatieprogrammatuur of de gegevensinfrastructuur.

Maatregel 5.

Antivirus-maatregelen kunnen bestaan uit:

- Het controleren van bestanden op de aanwezigheid van kwaadaardige programma's.
- Het detecteren van verdachte activiteiten (run-time) waarvan bekend is, dat ze door kwaadaardige programma's worden uitgevoerd.

Na detectie van een kwaadaardig bestand of programma is het mogelijk deze bestanden onschadelijk te maken of te vernietigen. Referentiebestanden van antivirus-maatregelen dienen regelmatig ververst te worden aangezien steeds nieuwe kwaadaardige programma's aangeboden worden (Overbeek, 2000).
De antivirus maatregelen zijn binnen STIS een elementaire maatregel ter bevordering van het relationeel vertrouwen. Een computervirusbesmetting veroorzaakt door een andere partij kan de data-uitwisseling lange tijd bemoeilijken.

**Encryptie**

Maatregel 6.

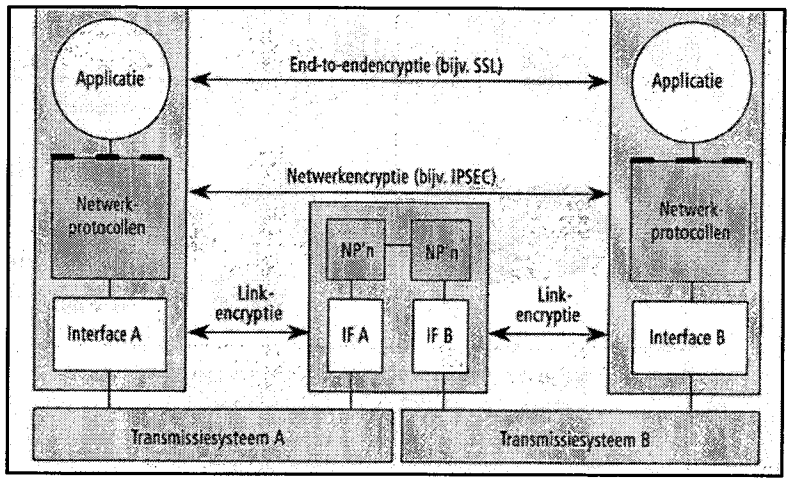
Voor de beveiliging van data-uitwisseling via interne en externe netwerken zijn cryptografische technieken onmisbaar (Overbeek, 2000). Op verschillende manieren kunnen deze technieken worden geïmplementeerd (Figuur 3-3), n.l.:

- Op applicatieniveau: De applicatie zorgt voor het uitwisselen van sleutelmateriaal en het vercijferen van de gegevens.
  Een voorbeeld hiervan is SSL (Secure Sockets Layer). SSL is een standaard protocol, dat door een applicatie kan worden gebruikt om een geauthentiseerde sessie op te zetten tussen een cliënt en een server. Tijdens deze sessie

worden cryptografische sleutels uitgewisseld en de sessie tussen de cliënt en de server wordt desgewenst vercijferd. SSL is een open protocol dat onafhankelijk is van applicatie of infrastructuur.

- Op netwerkniveau: De versleuteling vindt plaats buiten de applicatie om, door de netwerkprotocollen.
  Een voorbeeld hiervan is IPSEC (Internet Protocol Security) welk wordt toegepast indien Internet wordt gebruikt als VPN (Virtual Private Network). Bij het aanleggen van VPN's wordt gebruik gemaakt van 'encrypted tunneling'. Elk datapakketje wordt in een versleuteld IP-packet ingepakt. Bij de ontvanger wordt deze data met de bijbehorende unieke sleutel weer uitgepakt. Zo is het mogelijk via het 'onveilige' Internet en tegen lage kosten toch een veilige netwerkverbinding aan te leggen.
- Op linkniveau: De encryptie toegepast op de eindpunten van de fysieke communicatieverbinding wordt in de omgeving van de elektronische handel niet meer veel toegepast. Deze vorm van encryptie blijft ook voor STIS buiten beschouwing aangezien de eerdergenoemde vormen van encryptie een grotere flexibiliteit voor het beheer kennen.

**Bron: Overbeek, 2000**




**Figuur 3-3: Mogelijke encryptietechnieken in netwerken.**

Specifiek voor de versleutelingen op applicatieniveau wordt gebruik gemaakt van digitale handtekeningen. Een digitale handtekening is een waarmerk, die aan een bericht toegevoegd kan worden waaraan de ontvanger van het bericht kan zien, dat het bericht authentiek is gebleven nadat de handtekening is gezet. De digitale handtekening heeft dus een tweeledige functie:

- Vaststellen van de bron van het bericht (authenticatie);
- Vaststellen of het bericht ongeschonden is (integriteit).

In de bovengenoemde mechanismen kunnen digitale certificaten worden gebruikt voor authenticatie en sleuteluitwisseling. De uitgifte van certificaten is volgens paragraaf 3.4 een taak van de TTP (Trusted Third Party). Voor het laten slagen van de informatiebeveiliging op basis van encryptie speelt het beheer van sleutels en de PKI-infrastructuur (Public Key Infrastructure) een essentiële rol. Deze organisatorische facetten van de encryptie worden in de volgende paragraaf behandeld.

### *3.1.4 Organisatorische maatregelen*

Voor een deel van de beveiligingsmaatregelen zullen voorzieningen op organisatorisch vlak genomen moeten worden, willen deze technische maatregelen effect hebben (Overbeek, 2000). De maatregelen welke aanvullende organisatorische maatregelen vereisen, zijn de uitgifte van certificaten ten behoeve van encryptie en de PKI-infrastructuur.

**PKI-infrastructuur**

Een Public Key Infrastructure (PKI) is een organisatievorm, waarmee het toepassen van asymmetrische encryptie mogelijk gemaakt wordt, door het oplossen van de sleutelproblematiek. Hierbij wordt gebruik gemaakt van digitale certificaten, die door een Certification Authority (CA) uitgegeven worden. Een CA is een TTP, die zich specifiek richt op het beheren en het uitgeven van digitale certificaten. Een CA kan zijn diensten verlenen aan een besloten gemeenschap, zoals bij STIS het geval is.

Een digitaal certificaat is een combinatie van identiteit en openbare sleutel, die gewaarmerkt is door een CA. In dit certificaat is onder meer de volgende informatie opgenomen:

- De identiteit van de houder van het certificaat;
- De openbare sleutel van de houder;
- De identiteit van de CA, die het certificaat heeft afgegeven;
- De uiterste houdbaarheidsdatum van het certificaat.

Elk certificaat wordt door de CA, die het uitgeeft, gewaarmerkt met een digitale handtekening. De geldigheid van een certificaat kan worden gecontroleerd door het bericht te ontcijferen met de openbare (algemeen bekende) sleutel van de CA.

Het vertrouwen dat de gebruiker in een certificaat stelt, is volledig gebaseerd op het vertrouwen in de CA die het certificaat afgeeft. De betrouwbaarheid van de CA is van groot belang. De betrouwbaarheid van een CA moet blijken uit publieksverklaringen van de CA, zoals een Certification Practice Statement (CPS) en de Certificate Policies (CP), waarnaar de CA handelt (Overbeek, 2000).

Maatregel 7. Voor het vertrouwen in de data-uitwisseling van gevoelige gegevens binnen STIS, is het aan te bevelen een PKI-infrastructuur te implementeren, zodat de vertrouwelijkheid van dit type gegevens op berichtniveau gerealiseerd wordt.

**Certificatie**

Om het vertrouwen tussen organisaties te bevorderen, kan gebruik worden gemaakt van certificatie. Certificeren is een waarmerkingsproces dat er toe leidt dat een organisatie (of een product) een kwaliteitswaarmerk krijgt; een soort 'stempel van betrouwbaarheid'. Om dit te bereiken wordt de organisatie, die de certificering ondergaat, (of het product) getoetst aan een norm. Als de toetsing succesvol is, dan kan een certificaat uitgereikt worden als bewijsstuk (Overbeek, 2000).

Bij certificatie in het geval van STIS, is het object van onderzoek de beheersing van de informatiebeveiliging van die partij. Een adequate informatiebeveiliging vereist dat er binnen de betreffende organisatie een stelsel van uniforme spelregels wordt gehanteerd. Het managementsysteem dat hiervoor verantwoordelijk is, kan gecertificeerd worden. Een certificaat geeft zowel binnen een organisatie, als tussen organisaties, meer vertrouwen in de informatiebeveiliging van de

systemen waarmee de data-uitwisseling wordt gerealiseerd. Aangezien een certificaat alleen geldig blijft bij periodieke controles kunnen de andere partijen er beter op vertrouwen dat het beoogde niveau van beveiliging ook blijvend wordt geboden.

Sinds 1997 is het mogelijk, om op basis van de Code voor Informatiebeveiliging de informatiebeveiliging in een organisatie te laten certificeren door erkende organisaties. Binnen Nederland zijn de richtlijnen voor het certificeringsproces vastgelegd in het "Schema voor certificatie van informatiebeveiliging op basis van de Code voor Informatiebeveiliging" (BS7799), dat is ontwikkeld door het Stichting Instituut voor de bevordering van de keuring en Certificatie van Informatie Technologie (ICIT). Certificatie wordt internationaal erkend (Overbeek, 2000).

Maatregel 8. Certificatie is zinvol voor de deelnemende partijen aan STIS, welke de gevoelige data verwerken. Doorgaans zijn dit de grotere organisaties.

## 3.2 De opleiding en training

Maatregel 9. Een belangrijk deel van het relationeel vertrouwen ontstaat doordat een andere deelnemende partij aan STIS simpelweg de juiste handelingen met betrekking tot de data-uitwisseling uitvoert, welke op dat moment van haar verwacht worden. Om dit voor elkaar te krijgen is voldoende opleiding en training nodig in:

- het omgaan met de technische en organisatorische middelen om de data-uitwisseling tot stand te brengen;
- het nut en de noodzaak van de data-uitwisseling en welke rol de betreffende gebruiker daarin speelt.

Door het organiseren van opleiding en training zal het relationeel vertrouwen worden beïnvloed. Het relationeel vertrouwen wordt volgens de onafhankelijke variabele van het conceptuele model van STIS beïnvloed via de volgende aspecten: beheersing van de elementaire technieken en vaardigheden en consistentie in handelen (Ratnasingam, 2001). De opleidingen en trainingen beïnvloeden deze aspecten op positieve wijze. Hierdoor zal ook het relationeel vertrouwen in STIS vergroot worden.

## 3.3 De Interchange Agreement

Door het opstellen van een Interchange Agreement zal in beginsel het juridische vertrouwen worden beïnvloed. Het juridische vertrouwen wordt volgens de onafhankelijke variabele van het conceptuele model beïnvloed via het volgende aspect: het toepassen van standaarden als juridisch coördinatiemechanisme (Ratnasingam, 2001).
De inhoud van een Interchange Agreement beïnvloedt tevens het technologische en het relationeel vertrouwen. In de Interchange Agreement worden afspraken tussen de deelnemende partijen gemaakt over: vertrouwelijkheid, integriteit, authenticiteit, onweerlegbaarheid, toegangscontrole, beschikbaarheid en de toepassing van "Best practices". Hierdoor zal ook het technologische vertrouwen in STIS vergroot worden. Ter vergroting van het relationeel vertrouwen worden in een Interchange Agreement ook afspraken tussen de deelnemende partijen gemaakt over: de beheersing van de elementaire technieken en vaardigheden, consistentie in handelen (Ratnasingam, 2001).

Het opstellen van een Interchange Agreement beïnvloedt via de verschillende vormen van vertrouwen de participatie aan STIS op positieve wijze.

Bij de elektronische uitwisseling van gegevens treffen we een tweetal soorten van overeenkomsten aan:

- De Interchange Agreement — Een overeenkomst waarin de juridische aspecten van de elektronische uitwisseling van gegevens wordt geregeld.
- De onderliggende overeenkomst — De overeenkomst die tot stand komt door de uitwisseling van gegevens (de transactie).

### *3.3.1 De vormen van Interchange Agreements*

Partijen betrokken bij de elektronische handel, kunnen afzonderlijk bilaterale overeenkomsten of gezamenlijk een multilaterale overeenkomst sluiten.
Er zijn nadelen verbonden aan het sluiten van bilaterale overeenkomsten. Een partij zal met alle andere partijen waarmee zij elektronisch handel drijft, een aparte Interchange Agreement dienen te sluiten. In de situatie zijn dat een groot aantal partijen en dus onderhandelingen. Dit kost veel tijd en geld. Indien het aantal andere partijen groot is, kunnen de hierboven vermelde nadelen tot een onwerkbare situatie leiden. Een oplossing voor deze problematiek is de multilaterale overeenkomst. Een multilaterale overeenkomst is een meerpartijenovereenkomst[5], waarop de bepalingen betreffende wederkerige overeenkomsten van toepassing zijn[6].
In de situatie van STIS zal de groep van partijen kunnen fluctueren, dan is het raadzaam in een dergelijke multilaterale Interchange Agreement een toetredingsregeling en uittredingsregeling op te nemen
In de toetredingsregeling zal worden bepaald onder welke voorwaarden nieuwe partijen kunnen toetreden tot de Interchange Agreement. De toetredingsregeling mag niet in strijd zijn met het Nederlandse of Europese mededingingsrecht. Toetreding tot de Interchange Agreement leidt tot gebondenheid tussen de bestaande partijen en toetredende partij. Het is daarbij niet vereist dat de toetredende partij zich rechtstreeks tot de andere partijen bij de Interchange Agreement richt.
In de uittredingsregeling zal worden geregeld onder welke voorwaarden partijen uit de overeenkomst kunnen treden. De uittredende partij mag daarbij geen onredelijke voorwaarden voor uittreding worden opgelegd, daar ook dit in strijd kan zijn met het mededingingsrecht.

**Maatregel 10.** Voor het versterken van het vertrouwen in de data-uitwisseling van STIS is het streven naar een gelijkwaardige machtsverhouding tussen de deelnemende partijen een voorwaarde. Geen van de overheids- of commerciële partijen kan dus op basis van deze gelijkwaardigheid de voortrekkersrol nemen in het opstellen van bilaterale overeenkomsten. Voor het vertrouwen in STIS is daarom de multilaterale overeenkomst de aanbevolen vorm.

[5] in de zin van art. 6:279 BW

[6] uit Boek 6 BW

### *3.3.2 De onderwerpen in de Interchange Agreement*

In een Interchange Agreement kunnen een aantal onderwerpen betreffende de elektronische data-uitwisseling worden geregeld. Deze onderwerpen kunnen worden onderverdeeld in de volgende drie categorieën (Esch-2, 2002):

A. technische aspecten van de elektronische uitwisseling van gegevens;
B. beveiligingsaspecten van de elektronische uitwisseling van gegevens;
C. juridische aspecten van de elektronische uitwisseling van gegevens.

Hierna zal op deze verschillende categorieën nader worden ingegaan.

**A. De technische onderwerpen van de Interchange Agreement**

In een Interchange Agreement kunnen partijen vooraf afspraken maken over een aantal technische aspecten van de elektronische uitwisseling van gegevens. Naast de genoemde maatregelen met betrekking tot de informatiebeveiliging (paragraaf 3.1) kan worden gedacht aan:

1. de technieken, technische standaarden en versies, die partijen moeten gebruiken omwille van de compatibiliteit bij de onderlinge elektronische data-uitwisseling;
2. het testen bij implementatie van nieuwe (releases van) computerprogrammatuur die nodig is voor de elektronische data-uitwisseling;
3. back-up procedures bij het niet beschikbaar zijn van apparatuur, programmatuur of de diensten benodigd voor de elektronische data-uitwisseling.

Maatregel 11. In vele gevallen kan voor de regeling van de technische onderwerpen worden volstaan met kaderbepalingen, waarin naar een bijlage wordt verwezen voor de verdere uitwerking van deze aspecten. Deze bijlage maakt deel uit van de overeenkomst.

**B. De beveiligingsonderwerpen van de Interchange Agreement**

De Interchange Agreement kan een regeling opnemen die voorziet in het nemen van maatregelen ter beveiliging van de elektronische uitwisseling van gegevens. Hiermee conformeren alle deelnemende partijen van STIS zich formeel aan het gewenste niveau van informatiebeveiliging.

In geval van een geschil is het van belang te weten wat verstaan wordt onder een voldoende mate van beveiliging. Daarbij is de aard van de uit te wisselen gegevens, de omvang van de risico's en wat in de branche gebruikelijk is, van belang. Daarnaast zal het nemen van adequate beveiligingsmaatregelen van invloed zijn op de rechtspositie van partijen. Een elektronische registratie van een gegevensuitwisseling, zal meer bewijskracht bezitten, indien deze beveiligd is tegen manipulatie.

Maatregel 12. Voor STIS is het raadzaam, na te gaan welke beveiligingsmaatregelen voor de data-uitwisseling in de binnenvaartbranche als noodzakelijk worden geacht, zodat bij een eventueel dispuut de bewijskracht zo sterk mogelijk zal zijn.

**C. De juridische onderwerpen van de Interchange Agreement**

Naast de technische onderwerpen en de beveiligingsonderwerpen wordt in Interchange Agreements tevens een groot aantal juridische bepalingen opgenomen. Hieronder volgt een overzicht van bepalingen, welke voor STIS van toepassing zullen zijn.

*1. Het tijdstip en de plaats van tot stand komen van de onderliggende overeenkomst*

Voor het tot stand komen van een geldige onderliggende overeenkomst is het van belang eenduidigheid te verschaffen over de definities van 'het tijdstip van totstandkoming' en 'de plaats van totstandkoming'. Om aan deze onzekerheid

een einde te maken, kunnen partijen in de Interchange Agreement hierover een bepaling opnemen.

**Maatregel 13.** Binnen STIS kunnen de partijen overeenkomen dat:

- de onderliggende overeenkomst totstandkomt op het tijdstip dat de aanvaarding in de elektronische postbus van de aanbieder wordt gedeponeerd;
- de plaats waar de aanvaarding in de elektronische postbus van de aanbieder wordt gedeponeerd.

Een TTP kan voor de registratie zorgen van dit tijdstip en deze plaats.

*2. De ontvangstbevestiging*

De ontvangstbevestiging is een procedure, die partijen betrokken bij de elektronische data-uitwisseling in staat stelt om tijdig vast te stellen dat een bericht verloren gegaan of afgedwaald is. In de Aanpassingswet elektronische handel (Tweede Kamer-1, 2002) is de verplichting voor de leverancier opgenomen[7] om aan de afnemer zo spoedig mogelijk langs elektronische weg de ontvangst van de order te bevestigen. Ook is voorzien in een sanctie op het niet naleven van deze verplichting.

**Maatregel 14.** Aanvullend zou in de Interchange Agreement een regeling opgenomen moeten worden dat aan een elektronisch bericht geen rechtsgevolgen worden verbonden voordat de ontvangst van het bericht is bevestigd. Met deze afspraak verdelen zij het risico van het verloren gaan van de ontvangstbevestiging.

Tevens zal in de Interchange Agreement aangevuld moeten worden, dat het bevestigen van de ontvangst van een bericht niet betekent, dat de ontvanger van het bericht instemt met de inhoud van het bericht. Daarmee heeft de bevestiging van de ontvangst van een aanbod geen aanvaarding van dat aanbod tot gevolg.

Tenslotte moet de Interchange Agreement op dit gebied aangevuld worden met de bepaling, dat een door de afzender van een elektronisch bericht geregistreerde bevestiging van de ontvangst van dat bericht jegens de geadresseerde volledig bewijs oplevert van de ontvangst door geadresseerde van het bevestigde bericht tot op tegenbewijs. Daarmee krijgt de ontvangstbevestiging een grotere bewijskracht.

*3. De directe verwerking van berichten*

Elektronische berichten kunnen tegenwoordig snel worden verwerkt. Om financiële redenen kan een vertraging van de verwerking van berichten voordelen bieden. Zo kunnen afnemers van producten of diensten besluiten om hun bestellingen of opdrachten pas op het allerlaatste moment voor de fatale datum van levering van het product of verlening van de dienst te versturen. Dit stelt de afnemende partij in staat om kleinere voorraden aan te houden. Het uitstellen van het verzenden van elektronische berichten, zoals bestellingen of opdrachten tot dienstverlening, kan als nadeel hebben dat de organisatie steeds meer afhankelijk wordt van een tijdige verwerking van zijn berichten door de leverancier of de dienstverlener.

**Maatregel 15.** Partijen die het tijdstip van het verzenden van vitale berichten hebben verlaat in verband met de elektronische wijze van uitwisselen van gegevens, kunnen om die reden in de Interchange Agreement de verplichting voor de wederpartij opnemen om ontvangen elektronische berichten direct na ontvangst te verwerken.

[7] art. 6:227c lid 2 BW

*4. Gebreken in de berichtgeving*

Een elektronisch bericht kan verloren gaan, dubbel worden ontvangen, verminkt worden, afdwalen of met vertraging bij de geadresseerde aankomen. De wet biedt op dit vlak wel enig houvast.[8] Echter een aanvulling met behulp van de Interchange Agreement is voor dit onderwerp gewenst.

De vraag kan zich voordoen of een bericht dat gebrekkig is uitgewisseld, leidt tot gebondenheid.

Maatregel 16. In de Interchange Agreement kunnen de risico's verdeeld worden van een gebrekkige uitwisseling van elektronische berichten.

*5. De bevoegdheid van de afzender*

De herkomst van een elektronisch bericht kan nimmer met 100% zekerheid worden vastgesteld aan de hand van de elektronische handtekening die met een bericht is meegestuurd. Het is mogelijk dat een onbevoegde de beschikking heeft gekregen over de middelen voor het genereren van de elektronische handtekening en daarvan misbruik heeft gemaakt.
Dit blijft een onzekerheid welke tot juridische problemen kan leiden indien het bericht een rechtshandeling inhoudt. Indien het bericht afkomstig is van een derde die niet bevoegd is om voor en namens hem rechtshandelingen te verrichten is een (rechts-)persoon juridisch niet gebonden aan de rechtshandeling, verricht door middel van een elektronisch bericht (Esch-2, 2002). Dit is tevens het geval indien de houder van de handtekening de middelen ter beschikking heeft gesteld om voor en namens hem een elektronische handtekening te genereren. Daarmee kan de houder zijn vertegenwoordigingsbevoegdheid overschrijden.

In de Interchange Agreement kunnen betrokken partijen een andere regeling treffen, welke de aansprakelijkheid voor het misbruik of onbevoegd gebruikt van de elektronische handtekening regelt.

*6. Aansprakelijkheid*

De aan STIS deelnemende partijen kunnen in de Interchange Agreement de aansprakelijkheid voor schade ten gevolge van bepaalde gebeurtenissen of voor bepaalde vormen van schade uitsluiten of beperken.

Maatregel 17. Afhankelijk van de oorzaak kunnen ze:

- vastleggen dat zij jegens elkaar niet aansprakelijk zijn voor schade ten gevolge van een fout in de berichtgeving;
- de aansprakelijkheid voor economische schade uitsluiten of beperken tot een bepaald bedrag per gebeurtenis;
- het aansprakelijkheidsdomein inperken door contractueel bepaalde omstandigheden als overmacht te duiden. Denk bijvoorbeeld aan het niet of niet goed functioneren van het telecommunicatienetwerk, fouten van een intermediair ingeschakeld bij de uitwisseling van elektronische berichten of fouten in de programmatuur die wordt gebruikt bij het verzenden, ontvangen of verwerken van elektronische berichten.

[8] art. 3:37 BW

*7. Intermediairs*

**Maatregel 18.** Deelnemende partijen kunnen in de Interchange Agreement met betrekking tot intermediairs (denk aan TTP's) die zij inschakelen bij de uitwisseling van elektronische berichten, twee soorten bepalingen opnemen:

- Wie in hun onderlinge rechtsverhouding het risico van fouten van de intermediair dient te dragen.
- Waarin zij zich jegens elkaar verplichten om in de overeenkomst met de intermediair bepaalde verplichtingen op te leggen. Denk bijvoorbeeld aan de verplichting om bepaalde beveiligingsmaatregelen te treffen, om geheimhouding te betrachten ten aanzien van de inhoud van berichten of om te handelen in overeenstemming met de Wet Bescherming Persoonsgegevens.

*8. Logging*

**Maatregel 19.** In de Interchange Agreement kunnen verplichtingen opgenomen worden ten aanzien van de wijze van registratie en bewaring van uitgewisselde elektronische berichten en van de bewaartermijn. De kans op een geschil tussen partijen kan hierdoor worden verkleind. Zo zouden zij bijvoorbeeld kunnen afspreken dat de afzender en de ontvanger de elektronische berichten zullen bewaren in de vorm waarin deze zijn verstuurd respectievelijk ontvangen. De TTP kan hierin tevens een belangrijke functie vervullen.

*9. Bewijs*

**Maatregel 20.** In de Interchange Agreement kan een bewijsbepaling opgenomen worden waarin de volgende bewijsrechtelijke onderwerpen geregeld kunnen worden:

- De verdeling van de bewijslast;
- De toekenning van de bewijskracht van een geregistreerd bericht.

*10. Geheimhouding*

Zoals blijkt uit de problematiek van dit onderzoek kan een elektronisch bericht vertrouwelijke informatie bevatten. De vertrouwelijke informatie kan van dien aard zijn dat kennisneming daarvan door een onbevoegde derde schade kan berokkenen aan de afzender of de ontvanger. Het zal niet altijd mogelijk of gemakkelijk zijn om deze schade op geld te waarderen of het oorzakelijke verband tussen de geleden schade en de kennisneming van de vertrouwelijke informatie door de onbevoegde derde aan te tonen.

**Maatregel 21.** Naast de reeds beschreven maatregelen op het gebied van de informatiebeveiliging kunnen partijen in de Interchange Agreement:

- elkaar de verplichting opleggen om vertrouwelijke informatie geheim te houden;
- elkaar verplichten om maatregelen te nemen om het risico van kennisneming door onbevoegde derden te verminderen. Bij maatregelen kan bijvoorbeeld worden gedacht aan het in versleutelde vorm bewaren van ontvangen berichten.

De geheimhoudingsverplichting kan betrekking hebben op berichten die volgens de functionaliteit als vertrouwelijk zijn bestempeld.
Bij gebruikmaking van een TTP, zal in de overeenkomst met de intermediair een soortgelijke geheimhoudingsverplichting opgenomen worden.

*11. De bescherming van persoonsgegevens*

**Maatregel 22.** Elektronische data-uitwisseling kan betrekking hebben op persoonsgegevens. Partijen betrokken bij de elektronische data-uitwisseling, kunnen in de Interchange Agreement de volgende bepalingen opnemen:

- Aan elkaar de verplichting opleggen om de bepalingen uit de WBP (Wet Bescherming Persoonsgegevens) in acht te nemen. Voor STIS kan deze regeling in een Interchange Agreement van belang zijn, indien in de toekomst elektronische data-uitwisseling plaatsvindt met partijen uit landen die geen adequaat niveau van bescherming van persoonsgegevens kennen;
- Regelen wie de schade dient te dragen, indien er een ongeoorloofde verstrekking van persoonsgegevens plaatsvindt en dit leidt tot een schadeplicht ten opzichte van de persoon wiens gegevens het betreft;
- De maatregelen eisen, die partijen zullen treffen om de persoonsgegevens te beveiligen tegen ongeoorloofde kennisneming. Ook van een eventuele TTP worden soortgelijke maatregelen geëist.

*12. Geschillenbeslechting*

Maatregel 23. Deelnemende partijen kunnen in de Interchange Agreement een regeling opnemen voor de beslechting van geschillen.

*13. De looptijd en de beëindiging van de Interchange Agreement*

Maatregel 24. De Interchange Agreement kan worden aangegaan voor bepaalde of onbepaalde tijd. Indien de Interchange Agreement wordt aangegaan voor bepaalde tijd, kan de looptijd worden gekoppeld aan de termijn die deelnemende partijen nodig hebben om hun investeringen in apparatuur en programmatuur terug te verdienen.
In een Interchange Agreement voor onbepaalde tijd kan een opzeggingsregeling worden opgenomen. De opzegging wordt beheerst door de redelijkheid en de billijkheid.
Voorts kunnen partijen in de Interchange Agreement bepalen in welke gevallen een partij bevoegd is om de overeenkomst te ontbinden. Denk bijvoorbeeld aan de situatie dat de wederpartij failliet wordt verklaard.
In een multilaterale Interchange Agreement kunnen partijen afspreken welke gevolgen de opzegging van de overeenkomst door een van de partijen heeft voor de andere partijen. Zo kunnen zij overeenkomen dat de andere partijen in dat geval de overeenkomst onder dezelfde voorwaarden zullen voortzetten.

*14. De geldigheid van contractuele bedingen*

Maatregel 25. De opsteller van de Interchange Agreement dient ervoor te waken, dat de gestelde eisen redelijk en billijk blijven.

## 3.4 De Trusted Third Party (TTP)

De inzet van een TTP zal het relationeel vertrouwen beïnvloeden. Het relationeel vertrouwen wordt volgens de onafhankelijke variabele van het conceptuele model beïnvloed via het aspect: consistentie in handelen (Ratnasingam, 2001). Hierdoor zal het relationeel vertrouwen in STIS vergroot worden.
Het technologische vertrouwen wordt bij de inzet ven een TTP volgens de onafhankelijke variabele van het conceptuele model beïnvloed door de aspecten: vertrouwelijkheid, integriteit, authenticiteit, onweerlegbaarheid, toegangscontrole en de toepassing van "Best practices". Hierdoor zal het technologische vertrouwen in STIS vergroot worden (Ratnasingam, 2001).
De inzet van een TTP zal ook het juridische vertrouwen positief beïnvloeden. Door het bieden van een juridische zekerheid ten aanzien van registratie, ontvangstbevestiging en de uitgifte van elektronische handtekeningen (Esch-2, 2002). Hierdoor zal ook het juridische vertrouwen in STIS vergroot worden.

| Maatregel | Nr. | Behoefte | Gevraagde taak |
|---|---|---|---|
| Informatiebeveiliging | 1 | De uitgifte van elektronische handtekeningen. | Identificatie |
| | 2 | Het controleren van echtheid van de elektronische handtekeningen. | Authenticatie |
| | 3 | Het regelen van de toegang tot gevoelige gegevens, van deelnemende partijen aan STIS. | Autorisatie |
| | 4 | Het uitgeven en beheren van certificaten. | Certificatie |
| | 5 | Het stimuleren van interconnectiviteit en het bevorderen van het gebruik van standaarden | Standaardisatie |
| Interchange Agreement | 6 | De opslag van uitgewisselde berichten kan uitsluitsel geven in de bewijsvoering, in geval van een dispuut tussen deelnemende partijen. | Registreren/Opslag |
| | 7 | Het tijdstip en de plaats van totstandkoming van de onderliggende overeenkomst | Tijdstempelen |
| | 8 | De uitgifte van elektronische handtekeningen | Sleutelbeheer |

**Tabel 3-1: De taken van een TTP ten behoeve van STIS**

In het STIS Referentiemodel voor de Scheepvaart (AVV-1, 2001) wordt reeds gerefereerd naar de behoefte aan een rol van een informatiemakelaar of Trusted Third Party. Deze TTP kan faciliteren in de data-uitwisseling tussen de deelnemende partijen van STIS. Uit de bovenstaande Tabel 3-1 blijkt, dat er bij de implementatie van de maatregelen 'informatiebeveiliging' en 'Interchange Agreement' een aanvullende behoefte bestaat voor het inzetten van een onafhankelijke partij, welke een aantal specifieke taken voor zijn rekening neemt. Om redenen van vertrouwelijkheid kunnen deze taken niet bij een van de deelnemende partijen van STIS liggen.

Voor dit onderzoek zullen we de definitie van Duthler toepassen betreffende een Trusted Third Party:

> *'Een onafhankelijke, onpartijdige organisatie, die betrouwbaarheidsdiensten ten behoeve van het elektronische berichtenverkeer verleent.' (Duthler, 1998)*

Deze definitie van Duthler is bruikbaar, aangezien deze is opgesteld vanwege een onderzoek naar het verbeteren van de vertrouwensrelatie ten behoeve van de elektronische data-uitwisseling tussen deelnemende partijen met behulp van EDI.

Op basis van de benodigde functies (Tabel 3-1) kunnen voor een TTP de volgende taken worden geformuleerd:
1. identificatie, authenticatie en registratie;
2. autorisatie;
3. sleutelbeheer;
4. certificatie;
5. tijdstempelen;
6. registratie en bewaring;
7. stimuleren van interconnectiviteit en standaarden;

Maatregel 26. Voor het op een juiste wijze ten uitvoer brengen van bovengenoemde functies, zal de intermediair aan een aantal criteria moeten voldoen om zijn taken als een werkelijk Trusted Third Party te kunnen uitoefenen. Volgens Duthler voldoet de intermediair, zoals deze binnen STIS ingezet zal worden aan het beeld van de informatiemakelaar.
Voor een informatiemakelaar kunnen de volgende criteria geïdentificeerd worden:
1. Onpartijdigheid;
2. Onafhankelijkheid;
3. Continuïteit;
4. Deskundigheid;
5. Beveiliging.

De TTP kan voor STIS een aantal taken gaan invullen, waardoor het vertrouwen in de data-uitwisseling van STIS zal toenemen. Hiervoor zal een specifieke overeenkomst met een TTP opgesteld gaan worden.

## 3.5 De Aanpassingswet Elektronische Handel

De Europese Unie heeft sinds 1997 veel aandacht geschonken aan de ontwikkelingen betreffende de elektronische handel. In 1997 werd de consumentenbeschermende Richtlijn 'Overeenkomst op afstand' (EG-1, 1997) gepubliceerd. Vervolgens werd in 1999 de Richtlijn betreffende een gemeenschappelijk kader voor elektronische handtekeningen (EG-2, 2000) uitgebracht. Als laatste trad op 17 juli 2000 de Richtlijn inzake elektronische handel (EG-3, 2000) in werking. Uiterlijk op 17 januari 2002 had deze laatste richtlijn in de nationale wetgevingen van alle lidstaten geïmplementeerd moeten zijn. Voor Nederland heeft deze implementatie tot op heden niet plaatsgevonden. Na het zomerreces wordt deze aanpassingswet in de Tweede Kamer behandeld. Vervolgens zal de werkelijke implementatie van deze aanpassingswet gaan aanvangen.

De data-uitwisseling binnen STIS bevat maar voor een gedeelte transacties in economische zin; echter met de implementatie van de 'Aanpassingswet richtlijn inzake elektronische handel' zullen tevens een aantal tekortkomingen van de Nederlandse wetgeving worden ondervangen voor elektronische data-uitwisseling in het algemeen. De gevoeligheid van de 'Status van de elektronische transactie' wordt daarmee gelijk voor een groot deel weggenomen.
Op de volgende wijze wordt in de Aanpassingswet tegemoetgekomen voor de gevoeligheden van STIS:

- De geldige totstandkoming van een overeenkomst;
  De Wetgever stelt in art. 6:227a BW een viertal eisen om een overeenkomst die langs schriftelijke of elektronische weg tot stand gekomen is, rechtsgeldig te laten zijn:

1. De overeenkomst is raadpleegbaar door partijen;

Maatregel 27.

Volgens de Memorie van Toelichting (MvT) (Tweede Kamer-1 , 2002) van de Aanpassingswet dient de overeenkomst op dusdanige wijze te worden vastgesteld, dat de partijen in staat zijn om de inhoud daarvan ter latere kennisneming te ontsluiten en te bewaren. Voor STIS zou een TTP hierin een rol van betekenis kunnen spelen.

2. De authenticiteit van de overeenkomst is in voldoende mate gewaarborgd;

Maatregel 28.

Authentiek betekent 'echt'. De MvT stelt dat de partijen ter uitvoering van dit voorschrift de elektronische overeenkomst op zodanige wijze dienen vast te leggen, dat er in voldoende mate vertrouwd kan worden op de inhoud daarvan. Een hulpmiddel hierbij kan zijn het werken met elektronische handtekeningen. Voor de implementatie van deze eis binnen STIS zou een Trusted Third Party (TTP) een rol van betekenis kunnen spelen.

3. Het moment van totstandkoming van de overeenkomst kan met voldoende zekerheid worden vastgesteld;

Maatregel 29.

Volgens de MvT wordt het sluiten van een overeenkomst door middel van de standaard mechanismen van elektronische post niet voldoende geacht, aangezien deze mechanismen makkelijk gemanipuleerd kunnen worden. Ook voor de implementatie van deze eis binnen STIS lijkt voor een TTP een rol weggelegd. Hij kan onafhankelijk vaststellen of het contract tot stand gekomen is.

4. De identiteit van de partijen kan met voldoende zekerheid worden vastgesteld.

Voor STIS kan de elektronische handtekening goede diensten bewijzen bij het voldoen aan deze wettelijke eis. De implementatie vindt plaats in maatregel 30.

- De schriftelijke handelsdocumenten, waarin de eigendom van zaken of een vordering is belichaamd;

De Aanpassingswet biedt helderheid op dit vlak, aangezien wordt opgesomd, in welke gevallen een overeenkomst niet langs elektronische weg kan plaatsvinden. De vorige passage betreffende het tot stand komen van een overeenkomst is niet van toepassing op:

1. overeenkomsten die rechten doen ontstaan of overdragen ten aanzien van onroerende zaken, met uitzondering van huurrechten;
2. overeenkomsten waarbij persoonlijke of zakelijke zekerheden worden verstrekt door personen die niet handelen in de uitoefening van een beroep of bedrijf;
3. overeenkomsten waarvoor de wet de tussenkomst voorschrijft van de rechter, een overheidsorgaan of een beroepsbeoefenaar die een publieke taak uitoefent;
4. overeenkomsten die onder het familierecht of het erfrecht vallen.

Dit deel van de Aanpassingswet beschrijft eenduidig voor welke gevallen geen geldige overeenkomst gesloten kan worden. Voor overige handelsdocumenten is een elektronische uitvoeringsvorm mogelijk. Handelsdocumenten betreffende lading en vracht kunnen daarmee ook elektronisch worden uitgewisseld, hetgeen STIS daarmee kan implementeren.

- Het vaststellen van de identiteit en de bevoegdheid van de afzender;

Maatregel 30.

Zoals hierboven reeds opgemerkt, zal voor STIS de elektronische handtekening eenduidigheid geven betreffende de identiteit van afzender. De bevoegdheden zullen via de in te zetten TTP gehandhaafd moeten worden.

- De aansprakelijkheid voor fouten in de berichtgeving;

De onzekerheid betreffende de aansprakelijkheid voor fouten in de berichtgeving zal in de te sluiten Interchange Agreement weggenomen moeten worden. Zie hiervoor paragraaf 3.3. De implementatie van deze maatregel vindt reeds plaats via maatregel 17.

- De bewaring van transactieberichten;
  Voor STIS zou een TTP hierin een rol van betekenis kunnen spelen. Deze taak kan in de Interchange Agreement vast gelegd worden. Daarmee kan de TTP tevens een onafhankelijke rol gaan spelen voor de situatie dat er een onafhankelijk (elektronisch) bewijs geleverd moet worden, betreffende een geschil tussen deelnemende partijen aan STIS. Zie hiervoor paragraaf 3.3. De implementatie van deze maatregel vindt reeds plaats via maatregel 19.
- Het bewijs;
  Zoals bij vorig aandachtspunt reeds opgemerkt, kan, bij bestaande geschillen tussen deelnemers van STIS, door bewaring van transactieberichten, bewijsvoering worden geleverd door een TTP. Deze dient dan een onafhankelijke opstelling te hebben binnen de organisatie van STIS. Zie hiervoor paragraaf 3.3. De implementatie van deze maatregel vindt reeds plaats via maatregel 20.

De bovengenoemde uitleg betreffende de 'Aanpassingswet Richtlijn inzake elektronische handel' is gebaseerd op de publicaties van Gijrath & Kolthek (Gijrath & Kolthek, 2002) en der Klaauw-Koops (Klaauw-2, 2002).

Zodra de "Aanpassingswet richtlijn inzake elektronische handel" in werking treedt, zal een aantal onzekerheden uit bovengenoemde lijst wettelijk worden afgedekt. Voor de risico's blijft een aanvulling in de vorm van een overeenkomst ( Interchange Agreement) tussen deelnemende partijen vereist. Op welke wijze deze overeenkomst ingevuld kan worden is in paragraaf 3.3 aangegeven.

## 3.6 Conclusie

De maatregelen die genoemd zijn in dit hoofdstuk, zullen het vertrouwen in de data-uitwisseling van STIS vergroten. In dit hoofdstuk is uitsluitend toegelicht *waarom* ze van toepassing zijn op STIS. Het volgende hoofdstuk zal de wijze van implementatie (het *hoe*) in STIS adviseren.

In onderstaande tabel is een overzicht getoond, waarin alle mogelijke maatregelen voor STIS zijn opgesomd, en hoe deze van invloed zijn op de gevoeligheden van STIS.

| § | Maatregel | Omschrijving | Privacy | Bedrijf | Kwaliteit | Status transactie |
|---|---|---|---|---|---|---|
| **Informatiebeveiliging** | | | | | | |
| 3.1 | 1 | Backup maatregelen | - | - | X | - |
| | 2 | Uitwijkfaciliteiten organiseren | - | - | X | - |
| | 3 | Toegangsbeheersing | X | X | - | - |
| | 4 | Netwerkbeveiliging | X | X | - | X |
| | 5 | Antivirus maatregelen | - | - | X | - |
| | 6 | Encryptie op applicatie- of netwerkniveau incl. elektronische handtekening | X | X | X | X |

| | | | | | | |
|---|---|---|---|---|---|---|
| | 7 | PKI-infrastructuur | X | X | - | X |
| | 8 | Certificatie organisatie | X | X | X | - |
| **Opleiding en Training** | | | | | | |
| 3.2 | 9 | Opleiding en training | X | X | - | - |
| **Interchange Agreement** | | | | | | |
| 3.3 | 10 | Multilaterale overeenkomst | X | X | - | X |
| | 11 | Aanvullende technische onderwerpen | - | - | X | - |
| | 12 | Inventarisatie noodzakelijke beveiliging | - | - | - | X |
| | 13 | Tijdstip en plaats totstandkoming overeenkomst | - | - | - | X |
| | 14 | Afspraken over ontvangstbevestiging | - | - | - | X |
| | 15 | Directe verwerking van berichten | - | - | - | X |
| | 16 | Risicoverdeling bij gebreken in berichten | - | - | X | X |
| | 17 | Aansprakelijkheidsverdeling | - | - | X | X |
| | 18 | Inzet van intermediairs | - | - | - | X |
| | 19 | Loggingfaciliteiten | - | - | X | X |
| | 20 | Bewijs | - | - | X | X |
| | 21 | Geheimhouding | X | X | - | - |
| | 22 | Afspraken over persoonsgegevens | X | - | - | - |
| | 23 | Geschilbeslechting | - | - | X | X |
| | 24 | Looptijd en beëindiging IA | - | - | - | X |
| | 25 | De geldigheid van het contractuele beding | - | - | - | X |
| **Trusted Third Party** | | | | | | |
| 3.4 | 26 | Het inzetten van een TTP | X | X | X | X |
| **Aanpassingswet Elektronische Handel** | | | | | | |
| 3.5 | 27 | De inhoud van de overeenkomst ontsluiten en bewaren | - | - | - | X |
| | 28 | De authenticiteit van de overeenkomst borgen | - | - | - | X |
| | 29 | TTP stelt totstandkoming overeenkomst vast | - | - | - | X |
| | 30 | Bepalen identiteit en de bevoegdheid van de afzender | - | - | - | X |

**Tabel 3-2: Overzicht van de maatregelen, van invloed op de gevoeligheden van STIS.**

# 4 De aanbevelingen voor STIS

In het voorgaande hoofdstuk zijn een aantal mogelijke maatregelen genoemd welke door STIS ingezet kunnen worden ter vergroting van het vertrouwen in de elektronische data-uitwisseling. Deze maatregelen zullen de gevoeligheden van de data-uitwisseling elimineren; en daarmee het vertrouwen in de data-uitwisseling van STIS vergroten.
In dit hoofdstuk zal per gevoeligheid aangegeven worden welke maatregelen aanbevolen kunnen worden. Vervolgens wordt in dit hoofdstuk aangegeven welke partijen een rol van betekenis spelen in het implementeren van de aanbevolen maatregelen.

## 4.1 De gevoeligheden van de data-uitwisseling

In paragraaf 2.4.2 zijn de gevoeligheden van de data-uitwisseling binnen STIS genoemd. Middels het gericht implementeren van de maatregelen uit hoofdstuk 3 worden de soorten van vertrouwen (relationeel, technologisch en juridisch) uit het conceptueel model van STIS positief beïnvloed. Hierdoor wordt vervolgens de participatie aan STIS positief beïnvloed.
Aan geadviseerde maatregelen wordt steeds een gewicht toegekend, om de prioriteit van de maatregel aan te duiden.

Bij de uitwisseling van alle typen gevoeligheden is het relationeel, het technologische en het juridische vertrouwen (zie paragraaf 2.4.3) essentieel.
In het kader van het relationeel vertrouwen is het van belang, dat de andere partij, die de data behandelt consistentie toont in de goede behandeling van deze gegevens.
In het kader van het technologische vertrouwen is het van belang, dat de partijen, die de data verwerken, goede voorzieningen treffen, die misbruik van deze gegevens voorkomt.
In het kader van het juridische vertrouwen is het van belang, dat de partijen, die de data verwerken, formeel hebben vastgelegd hoe ze onderling omgaan met deze data. Dit in aanvulling op de bestaande wetgeving betreffende dit gebied.
Op basis van deze bovenstaande constatering komen de volgende maatregelen in aanmerking voor implementatie, zodat de gevoeligheid met betrekking tot de privacygevoelige gegevens geminimaliseerd wordt.

| Maat-regel | Omschrijving | Privacy | Bedrijf | Kwaliteit | Status transactie |
|---|---|---|---|---|---|
| | **Informatiebeveiliging** | | | | |
| 1 | Backup maatregelen | - | - | Laag | - |
| 2 | Uitwijkfaciliteiten organiseren | - | - | Laag | - |
| 3 | Toegangsbeheersing | Hoog | Hoog | - | - |
| 4 | Netwerkbeveiliging | Hoog | Hoog | - | Laag |
| 5 | Antivirus maatregelen | - | - | Laag | - |
| 6 | Encryptie op applicatie- of netwerkniveau incl. elektronische handtekening | Hoog | Hoog | Hoog | Hoog |
| 7 | PKI-infrastructuur | Hoog | Hoog | - | Hoog |

| | | | | | |
|---|---|---|---|---|---|
| 8 | Certificatie organisatie | Laag | Laag | Hoog | - |
| **Opleiding en Training** | | | | | |
| 9 | Opleiding en training | Laag | Laag | - | - |
| **Interchange Agreement** | | | | | |
| 10 | Multilaterale overeenkomst | Laag | Laag | - | Laag |
| 11 | Aanvullende technische onderwerpen | - | - | Laag | - |
| 12 | Inventarisatie noodzakelijke beveiliging | - | - | - | Hoog |
| 13 | Tijdstip en plaats totstandkoming overeenkomst | - | - | - | Hoog |
| 14 | Afspraken over ontvangstbevestiging | - | - | - | Hoog |
| 15 | Directe verwerking van berichten | - | - | - | Hoog |
| 16 | Risicoverdeling bij gebreken in berichten | - | - | Hoog | Hoog |
| 17 | Aansprakelijkheidsverdeling | - | - | Hoog | Hoog |
| 18 | Inzet van intermediairs | - | - | - | Hoog |
| 19 | Loggingfaciliteiten | - | - | Hoog | Hoog |
| 20 | Bewijs | - | - | Hoog | Hoog |
| 21 | Geheimhouding | Hoog | Hoog | - | - |
| 22 | Afspraken over persoonsgegevens | Hoog | - | - | - |
| 23 | Geschilbeslechting | - | - | Hoog | Hoog |
| 24 | Looptijd en beëindiging IA | - | - | - | Hoog |
| 25 | De geldigheid van het contractuele beding | - | - | - | Hoog |
| **Trusted Third Party** | | | | | |
| 26 | Het inzetten van een TTP | Hoog | Hoog | Laag | Hoog |
| **Aanpassingswet Elektronische Handel** | | | | | |
| 27 | De inhoud van de overeenkomst ontsluiten en bewaren | - | - | - | Hoog |
| 28 | De authenticiteit van de overeenkomst borgen | - | - | - | Hoog |
| 29 | TTP stelt totstandkoming overeenkomst vast | - | - | - | Hoog |
| 30 | Bepalen identiteit en de bevoegdheid van de afzender | - | - | - | Hoog |

**Tabel 4-1: Totaaloverzicht van de maatregelen ter bevordering van het vertrouwen in de data-uitwisseling van STIS.**

In de bovenstaande tabel zijn prioriteiten toegekend aan de inzet van de maatregelen, ten behoeve van een bepaalde vorm van gevoeligheid.
Daar waar de kwalificatie "Hoog" is toegekend, is het zeer aan te bevelen dat de maatregel wordt uitgevoerd. De vergroting van het vertrouwen is met het uitvoeren van de maatregel naar verwachting groot.
Bij een kwalificatie "Laag" is de implementatie gewenst, maar niet noodzakelijk. De vergroting van het vertrouwen is met het uitvoeren van de maatregel naar verwachting beperkt.
Indien de kwalificatie "-" is toegekend heeft de maatregel geen invloed op de betreffende gevoeligheid. Het uitvoeren van de maatregel zal geen vergroting van het vertrouwen tot gevolg hebben.

## 4.2 De implementatie van de maatregelen door de diverse partijen

De maatregelen zoals deze in Tabel 4-1 zijn opgesomd hebben steeds betrekking op een beperkt aantal partijen binnen STIS. In deze paragraaf wordt aangegeven welke (groep van) partijen met deze maatregelen aan de slag moet.

In paragraaf 1.3.4 zijn de typen deelnemende partijen aan STIS opgesomd. Daarnaast zijn er een aantal taken welke door geen van deze partijen individueel uitgevoerd kunnen worden, omwille van het onderlinge vertrouwen. Voorbeelden van deze taken zijn:

- Het opstellen en opleggen van de Interchange Agreement aan de deelnemende partijen van STIS;
- Het contracteren en het aansturen van een TTP;
- Het vaststellen van nieuwe (technische) standaarden;

Voor deze taken dient een groep van afgevaardigden gekozen worden uit de deelnemende partijen van STIS. De belangen van de deelnemende partijen aan STIS zullen door middel van een evenwichtige samenstelling van deze groep behartigd moeten worden. Voor dit onderzoek zal de naam van deze groep worden vastgesteld als de "regiegroep STIS".

### *4.2.1 Privacygevoelige gegevens*

De partijen welke maatregelen dienen te treffen met betrekking tot de privacygevoelige gegevens, zijn over het algemeen de grotere bedrijven. De privacy van de individuele schipper is hier in het geding. Alle partijen welke regelmatig gedurende de reis van een schip data uitwisselen met dit schip, of hiervan data verzamelen, verwerken privacygevoelige gegevens. Deze partijen zijn de overheidspartijen en de grotere marktpartijen.

Deze partijen dienen extra aandacht te besteden aan maatregelen tot informatiebeveiliging, zodat geen onbevoegden toegang kunnen krijgen tot de privacygevoelige data (maatregel 3, 4, 6).
Binnen deze organisaties zullen aanvullende procedures ter ondersteuning van de informatiebeveiliging geïmplementeerd moeten worden (maatregel 7 en 8). Tevens zal door middel van opleiding en training het belang en de werkwijze van deze maatregelen onder de aandacht gebracht moeten worden (maatregel 9).

Bovengenoemde maatregelen worden door de deelnemende partijen aan STIS individueel geïmplementeerd. De verplichting hiertoe kan in de Interchange Agreement opgenomen worden.

De regiegroep STIS zal relevante passages in de Interchange Agreement moeten opnemen met betrekking tot de geheimhouding en correcte behandeling van dit type van gegevens (maatregel 21 en 22). Tevens zal deze regiegroep een TTP inzetten om de toegang tot deze gevoelige gegevens te handhaven (maatregel 26). Voor de beheersbaarheid en de uniformiteit van de af te sluiten Interchange Agreement, kan de regiegroep kiezen voor het type multilaterale overeenkomst (maatregel 10).

### *4.2.2 Bedrijfsgevoelige gegevens*

De partijen welke maatregelen dienen te treffen met betrekking tot de bedrijfsgevoelige gegevens, zijn over het algemeen de grotere bedrijven. De gegevens waaruit het bedrijfsmatig handelen van de individuele schipper is af te leiden, zijn relevant voor dit type van gevoeligheid. Alle partijen welke regelmatig

gedurende de reis van een schip data uitwisselen met dit schip, of hiervan data verzamelen, verwerken dit type van gegevens. Deze partijen zijn de overheidspartijen en de grotere marktpartijen.

Deze partijen dienen extra aandacht te besteden aan maatregelen tot informatiebeveiliging, zodat geen onbevoegden toegang kunnen krijgen tot de bedrijfsgevoelige data (maatregel 3, 4, 6).
Binnen deze organisaties zullen aanvullende procedures ter ondersteuning van de informatiebeveiliging geïmplementeerd moeten worden (maatregel 7 en 8). Tevens zal door middel van opleiding en training het belang en de werkwijze van deze maatregelen onder de aandacht gebracht moeten worden (maatregel 9).

Bovengenoemde maatregelen worden door de deelnemende partijen aan STIS individueel geïmplementeerd. De verplichting tot het implementeren van deze maatregelen kan in de Interchange Agreement opgenomen worden.

De regiegroep STIS zal relevante passages in de Interchange Agreement moeten opnemen met betrekking tot de geheimhouding van dit type van gegevens (maatregel 21). Tevens zal deze regiegroep een TTP inzetten om de toegang tot deze gevoelige gegevens te handhaven (maatregel 26). Voor de beheersbaarheid en de uniformiteit van de af te sluiten Interchange Agreement, kan de regiegroep kiezen voor het type multilaterale overeenkomst (maatregel 10).

### *4.2.3 Kwaliteit van de nautische gegevens*

De partijen welke maatregelen dienen te treffen met betrekking tot de kwaliteit van de nautische gegevens, zijn over het algemeen de vaarwegbeherende (overheids-)organisaties. De kwaliteit en de beschikbaarheid van deze gegevens kan geborgd worden door de maatregelen 1, 2, 5, 6, 8 en 11.
Binnen deze organisaties zullen aanvullende procedures ter ondersteuning van de informatiebeveiliging geïmplementeerd moeten worden (maatregel 8).

De regiegroep STIS zal relevante passages in de Interchange Agreement moeten opnemen met betrekking tot de risicoverdeling bij gebrekkige berichtgeving en de daarbij behorende aansprakelijkheidsverdeling (maatregel 16 en 17). In geval van een optredend geschil zal door middel van logging de bewijsvoering worden gevoed (maatregel 19, 20 en 23). Mogelijk kan hierbij een rol voor de TTP zijn weggelegd volgens maatregel 26.

### *4.2.4 De status van de elektronische transactie*

De partijen welke maatregelen dienen te treffen om de status van de elektronische transactie te waarborgen, zijn de grote commerciële bedrijven welke overeenkomsten sluiten via het berichtenverkeer van STIS. Dit berichtenverkeer vindt plaats tussen schipper en diverse marktpartijen. De maatregelen zullen grotendeels door de grotere marktpartijen worden geïmplementeerd (maatregel 4, 6 en 7). De schippers zullen zich kunnen beperken tot het in bezit komen van een elektronische handtekening en de juiste applicatiesoftware (maatregel 6 en 7).
Bovengenoemde maatregelen worden door de deelnemende partijen aan STIS individueel geïmplementeerd. De verplichting tot het implementeren van deze maatregelen kan in de Interchange Agreement opgenomen worden.

De regiegroep STIS dient een groot scala van relevante passages in de Interchange Agreement opnemen, zodat de tekortkomingen van de wetgevingsinstrumenten worden afgedekt (maatregel 12, 13, 14, 15, 16, 17, 18, 19, 20, 23, 24 en 25). Voor de beheersbaarheid en de uniformiteit van de af te sluiten Interchange Agreement, kan de regiegroep kiezen voor het type multilaterale overeenkomst (maatregel 10). Tevens zal deze regiegroep een TTP inzetten om het berichtenverkeer rond de transacties te faciliteren (maatregel 26).

De Trusted Third Party (TTP) heeft een aantal specifieke taken met betrekking tot de overeenkomsten , voortkomend uit de transacties (maatregel 27, 28, 29 en 30). Deze maatregelen kunnen echter pas worden geïmplementeerd, zodra de Aanpassingswet Elektronische Handel van kracht is.

## 4.3 Conclusie

Met het toewijzen van de maatregelen aan de betreffende gevoeligheden van de data-uitwisseling kunnen de maatregelen worden geïmplementeerd door de relevante partijen welke betrokken zijn bij deze gevoelige data-uitwisseling.

Een aantal van de aanbevolen maatregelen zullen een grote inspanning en voorbereidingstijd vergen, alvorens de maatregelen geïmplementeerd kunnen worden. Rekening houdende met de STIS-implementatie voor 2005, is de beschikbare tijd beperkt. Samen met de heersende financiële krapte bij de Nederlandse overheid zullen er prioriteiten aan de maatregelen moeten worden toegekend. Een aantal van de maatregelen vergen dus aandacht op de korte termijn. Op basis van deze afweging kan een prioriteitenlijst worden opgesteld voor het totaalpakket aan maatregelen:

1. In overleg met relevante deelnemers aan STIS, overeenstemming bereiken over de inhoud van de Interchange Agreement op hoofdlijnen;
2. Het starten van een onderzoek naar het vereiste takenpakket van een Trusted Third Party binnen STIS;
3. Het starten van een onderzoeken naar het vereiste niveau van informatiebeveiliging in het kader van STIS.

Op basis van deze onderzoeken en afstemming kunnen de meer gedetailleerde maatregelen uit Tabel 4-1 geïmplementeerd worden.

Met deze uitwerking van hoofdstuk 4 wordt de laatste deelvraag van dit onderzoek beantwoord, en daarmee tevens de probleemstelling van dit onderzoek.

# Literatuur


1. **AVV-1**: *STIS Referentiemodel voor de scheepvaart*, Tussenrapportage FS/FO, versie 1.0, Ministerie van Verkeer en Waterstaat, Rijkswaterstaat, Adviesdienst Verkeer en Vervoer, Project STIS, april 2001.
2. **AVV-2**: *STIS opzet functionele architectuur*, Ministerie van Verkeer en Waterstaat Rijkswaterstaat, Adviesdienst Verkeer en Vervoer, Project STIS, april 2001.
3. **Duthler**, *Met recht een TTP!*, Mr. Drs. A.W. Duthler, ITeR-reeks nr.11, Kluwer, Deventer, ISBN 90-14-0577-68, 1998.
4. **EG-1**, PbEG 1997 L 144/19, *Richtlijn 97/7/EG betreffende de bescherming van de consument bij op afstand gesloten overeenkomsten.*
5. **EG-2**, PbEG 2000 L 13/12, *Richtlijn 1999/93/EG van het Europese Parlement en van de Raad van 13 december 1999 betreffende een gemeenschappelijk kader voor elektronische handtekeningen.*
6. **EG-3**, PbEG 2000 L 178/1, *Richtlijn 2000/31 /EG van het Europese Parlement en de Raad van 8 juni 2000 betreffende bepaalde juridische aspecten van de diensten van de informatiemaatschappij, met name de elektronische handel, in de interne markt.*, Verder Richtlijn inzake elektronische handel.
7. **Esch-1**: *Electronic data interchange (EDI) en het vermogensrecht*,. Mr. R.E. van Esch, W.E.J. Tjeenk Willink, Deventer, ISBN 90-271-5047-8, 1999.
8. **Esch-2**: *De overeenkomst als reguleringsinstrument*, uit: Recht en elektronische handel, Prof. Mr. R.E. van Esch en Prof. Mr. J.E.J. Prins, Recht en Praktijk nr. 68, Kluwer, Deventer, ISBN 90-268-4022-5, 2002.
9. **Franken et. al.**: *Recht en computer*, Prof. Mr. H, Franken, Prof. Mr. H.W.K. Kaspersen en Mr. A.H. de Wild, Kluwer, Deventer, ISBN 90-268-3638-4, 2001.
10. **Gijrath & Kolthek**, *Wetsvoorstel Elektronische Handel: Gemiste kansen bij elektronisch contracteren?*, S.J.H. Gijrath en R.J. Kolthek, in: Computerrecht, nr. 6, pag. 352 – 360, 2002.
11. **Klaauw-1**: *Praktisch informaticarecht voor het Hoger Beroeps Onderwijs*, Mr. F.A.M. van der Klaauw-Koops en Mr. S.F.M. Corvers, W.E.J. Tjeenk Willink, Zwolle, ISBN 90-271-4239-4, 1995.
12. **Klaauw-2**: *Het totstandkomen van elektronische contracten*, uit: Recht en elektronische handel, Prof. Mr. R.E. van Esch en Prof. Mr. J.E.J. Prins, Recht en Praktijk nr. 68, Kluwer, Deventer, ISBN 90-268-4022-5, 2002.
13. **Kuiters-Goederen**: Interview: *Vertrouwen betreffende elektronische data-uitwisseling in de Nederlandse binnenvaartsector*, Rijkswaterstaat, Adviesdienst Verkeer en Vervoer, Project STIS, Rotterdam, 14-1-2002.
14. **Mayer et. al.**: *An Integrative Model of Organizational Trust*, Mayer, R.C., Davis, J.H., and Schoorman, F.D., uit: Academy of Management Review., 20, 3, pag. 709-734, 1995.
15. **Overbeek et. al.**: *Informatiebeveiliging onder controle*, Paul Overbeek, Edo Roos Lindgreen, Marcel Spruit, Pearson Education Uitgeverij B.V., Amsterdam, ISBN 90-430-0289-5, 2000.
16. **Ratnasingam**: *Interorganisational trust in business to business E-commerce*, Pauline Puvanasvari Ratnasingam, Erasmus Research Institute of Management (ERIM), Rotterdam, ISBN 90-5892-017-8, 2001.

17. **Stuurman en Wijnands**: *Een privaatrechterlijk kader voor EDI*, uit: Electronic Commerce, ITeR-reeks nr.12, Kluwer, Deventer, ISBN 90-268-3322-9, 1998.
18. **Tanenbaum**: *Computernetwerken*, Andrew S. Tanenbaum, Academic Service, Schoonhoven, ISBN 90-395-0557-8, 1999.
19. **Tweede Kamer-1**, Kamerstukken 11 2001/02, 28 197, *Aanpassing van het Burgerlijk Wetboek, het Wetboek van Burgerlijke Rechtsvordering, het Wetboek van Strafrecht en de Wet op de economische delicten ter uitvoering van richtlijn nr. 2000/31/EG van het Europees Parlement en de Raad van de Europese Unie van 8 juni 2000 betreffende bepaalde juridische aspecten van de diensten van de informatiemaatschappij, met name de elektronische handel, in de interne markt (PbEG L 178),* verder Aanpassingswet richtlijn inzake elektronische handel, nrs.1-7, SDU Uitgevers, Den Haag, 2002.
20. **van Bellen**: *Van EDI naar elektronische handel*, uit: Recht en elektronische handel, Prof. Mr. R.E. van Esch en Prof. Mr. J.E.J. Prins, Recht en Praktijk nr. 68, Kluwer, Deventer, ISBN 90-268-4022-5, 2002.
21. **Vlist et. .al.**: *EDI in de transportsector*, Prof. Ir. P. van der Vlist, W.J. de Jong, A.E. Kolff, Drs. D.J. van der Net, Drs. Ing. A. van Overbeek, A.T.C. Siebbeles, Samson Bedrijfsinformatie, Alphen aan de Rijn / Zaventem, ISBN 90-14-04638-3, 1994.
22. **Vries**: *Goederenvervoer over water*, C.J. de Vries, Van Gorcum, Assen, ISBN 90 232 3549 5, 2000.
23. **V&W-1**: Nationaal Verkeers- en Vervoerplan 2001-2020; Uitwerking voorgenomen beleid voor veilige en vlotte scheepvaart op de binnenwateren, *Vaarplan 2001-2005*, Ministerie van Verkeer en Waterstaat Directoraat-Generaal Goederenvervoer, Den Haag, 2001.
24. **V&W-2**: *Varen in de digitale delta*, Nienke Bagchus, Ministerie van Verkeer en Waterstaat, Directoraat Generaal Goederenvervoer, Rotterdam, augustus 2001.

# Bijlage 1: Gebruikte afkortingen

| | |
|---|---|
| CA | Certification Authority |
| CP | Certificate Policies |
| CPS | Certification Practice Statement |
| DSA | Digital Signature Algorithm |
| E-commerce | E-commerce |
| E-mail | Electronic Mail |
| EDI | Electronic Data Interchange |
| EDIFACT | EDI for Administration, Commerce and Transport |
| IA | Interchange Agreement |
| ICIT | Stichting Instituut voor de bevordering van de keuring en Certificatie van Informatie Technologie |
| ICT | Informatie- en CommunicatieTechnologie |
| IPSEC | Internet Protocol Security |
| IT | InformatieTechnologie |
| IVR | Internationaal Vaartuigen Register |
| IVS90 | Informatie- en Volgsysteem Scheepvaart |
| MvT | Memorie van Toelichting |
| NVVP | Nationaal Verkeer en VervoersPlan |
| PKI | Public Key Infrastructure |
| RIS | River Information Services |
| Rv | Wetboek van Burgerlijke Rechtsvordening |
| RWS | Rijkswaterstaat |
| SLA | Service Level Agreement |
| SSL | Secure Sockets Layer |
| STIS | Scheepvaart Transport Informatie Services |
| TEMA | Techniek en Maatschappij |
| TTP | Trusted Third Party |
| UMTS | Universal Mobile Telecommunications System |
| V&W | Ministerie van Verkeer en Waterstaat |
| VAN | Value Added Network |
| VPN | Virtual Private Network |
| WBP | Wet Bescherming Persoonsgegevens |

# Bijlage 2: Definities van vertrouwen

(Bron: Ratnasingam, 2001)

| Bron | Discipline | Definities van vertrouwen (Trust) |
|---|---|---|
| Anderson and Narus (1990) | Marketing | A firm's belief that another company will perform actions that will result in positive outcomes for the firm, as well as not taking unexpected actions that would result in negative outcomes for the firm. |
| Barney and Hansen (1994) | Management | Mutual confidence that no party in an exchange will exploit one another's vulnerabilities. |
| Bromiley and Cummings (1992) | Management | Expectation that another individual or group will (1) have good faith and make efforts to behave in accordance with any commitments, both explicit or implicit, (2) be honest in whatever negotiations preceding those commitments, and (3) not take excessive advantage of others even when the opportunity (to renegotiate) is available. |
| Deutsch (1958) | Sociology | Actions that increase one's vulnerability to the other. |
| Doney and Cannon(1997) | Psychology | Perceived credibility and benevolence of a target of trust. |
| Dyer and Chu (2000) | Management | One party's confidence that the other party in the exchange relationship will not exploit its vulnerabilities. |
| Fukuyama (1995) | Sociology | Exceptions that arise within a community of regular, honest and cooperative parties, based on commonly shared norms, on the part of other members of that community. |
| Gabarro (1987) | Management | Consistency of behavior such that judgement about trust in working relationships is based on the accumulation of interactions, specific incidents, problems, and events. |
| Gambetta (1988) | Sociology | Probability that one economic actor will make decisions and take actions that will be beneficial or at least not detrimental to another. |
| Ganesan (1994) | Marketing | Willingness to rely on an exchange partner in confidence. |
| Hosmer (1995) | Management | Expectation by one person, group, or firm upon voluntarily accepted duty on the part of another person, group, or firm to recognize and protect the rights and interests of all others engaged in a joint endeavor or economic exchange. |
| Keen (1999) | Information Systems and Management | Confidence in the business relationship. The definition is extended to include risk, and it focuses on the relationships that directly involve computers and telecommunications thus creating a trust bond (security, safety, honesty, consumer-protection laws, contracts, privacy, reputation. brand, mutual self-interest). |

| | | |
|---|---|---|
| Kumar (1996) | Marketing and Management | Trust is stronger than fear. Partners that trust each other generate greater profits, serve customers better, and are more adaptable. |
| Lewicki and Bunker (1996) | Management and Sociology | A state involving confident, positive expectation about another's motives with respect to oneself in situations entailing risk. |
| Lewis and Weigert (1986) | Sociology | Undertaking of a risky course of action on the confident expectation that all persons involved in the action will act competently and dutifully. |
| Mayer, Davis and Schoorman (1995) | Management | Willingness of a party to be vulnerable to the actions of another party based on the expectation that the other will perform a particular action important to the trustor, irrespective of the ability to monitor or control that other party. |
| McAllister (1995) | Management | Cognition based on the concept that we choose whom we will trust, in what respects, and under what circumstances: affective foundations of trust consist of emotional bonds between trading partners. |
| Mishra (1996) | Management | A party's willingness to be vulnerable to another party based on the belief that the latter party is (1) competent, (2) open, (3) concerned and (4) reliable. |
| Moorman, Deshpande and Zaltman (1993) | Marketing | Willingness to rely on an exchange partner with whom one has confidence. Also trust has been viewed as (1) a belief, sentiment or expectation: and as (2) a behavioral intention that reflects reliance on trading partners and involves vulnerability and uncertainty on the part of the trustor. |
| Morgan and Hunt (1994) | Management | Trust exists when one party has confidence in an exchange partner's reliability and integrity. |
| 0' Brien (1995) | Management | An expectation about the positive actions of other people, without being able to influence or monitor the outcome. |
| Ring and Van de Ven (1994) | Management | Trust as confidence implies: (1) the behavior of another will conform to one's expectation, and (2) the goodwill of another. |
| Sabel (1993) | Psychology | The mutual confidence that no party to an exchange will exploit the other's vulnerability. Trust is today widely r aided as a condition for competitive success. |
| Sako (1998) | Sociology | An expectation held by an agent that its trading partner will behave in a mutually acceptable manner (including an expectation that neither party will exploit the other's vulnerabilities). |
| Schurr and Ozane (1987) | Marketing | The belief that a party's word or promise is reliable and a will fulfill its oblations in an exchange relationship. |
| Zucker (1986) | Sociology | A set of logical expectations shared by everyone involved in an economic exchange. |

# Bijlage 3: Rollen in de binnenvaart

| | Rol | Taak | Omschrijving |
|---|---|---|---|
| 1 | Expediteur aanbodzijde | Acquisitie | Het werven van klanten en opdrachten |
| | | Indicatieve planning | Het maken van een planning voordat de schipper de reis aanneemt, waarbij de randvoorwaarden voor de reis meegenomen worden. |
| | | Match | De overeenkomen van vraag en aanbod |
| | | Boeken/reserveren | Het daadwerkelijk boeken van de reis bij een bepaalde schipper. |
| | | Vooraanmelding | - |
| 2 | Vrachtbemiddelaar | Acquisitie | Het werven van klanten en opdrachten |
| | | Indicatieve planning | Het maken van een planning voordat de schipper de reis aanneemt, waarbij de randvoorwaarden voor de reis meegenomen worden. |
| | | Match | De overeenkomen van vraag en aanbod |
| | | Boeken/reserveren | Het daadwerkelijk boeken van de lading bij de schipper. |
| | | Vooraanmelding | - |
| | | Volgen lading | Het bijhouden wat de status van de lading is (waar en op welk tijdstip en in welke conditie de lading zich bevindt) |
| 3 | Gezagvoerende schipper | Bewaken conditie schip | Het bekijken en vastleggen van de omstandigheden op het schip en zonodig onderhoud plegen. |
| | | Proviand, bunkeren | Het inslaan van benodigde proviand en brandstof voor een reis. |
| | | Operationele pre-trip planning | Het maken van een definitief vaarplan, rekening houdend met planning van terminals en verwachtingen t.a.v. de verkeerssituatie langs de af te leggen route. |
| | | Operationele on-trip planning | Het aanpassen van de operationele pre-trip planning tijdens de reis op basis van de feitelijke gebeurtenissen. |
| | | Vooraanmelding | Het doorgeven van de geplande reis aan de terminal (stuwadoor) |
| | | Bewaken kwaliteit en kwantiteit bemanning | Het bekijken en vastleggen van het aantal bemanningsleden en het niveau van kennis en vaardigheden van deze bemanning. |
| | | Bewaken combinatie schip / lading | Het vastleggen van scheepskenmerken en ladingkenmerken om de veiligheid van de combinatie hiervan te garanderen. |
| 4 | Navigatie ondersteunende dienst | Bestellen / boeken | Het ontvangen en verwerken van bestellingen van derden om gebruik te maken van nautische diensten. |
| | | Plannen / reserveren | Het plannen en reserveren van faciliteiten om de navigatie van het schip mogelijk te maken (loods, sleper). |
| | | Uitvoeren | Het begeleiden van het schip (slepen, loodsen) |

| | Rol | Taak | Omschrijving |
|---|---|---|---|
| 5 | Hulpdienst | Bergen | Het bergen van schip, lading en bemanning in geval een calamiteit optreedt. |
| | | Calamiteitenbestrijding | Het pro-actief, preventief en repressief bestrijden van calamiteiten en het verlenen van nazorg in geval een calamiteit optreedt. |
| 6 | Bemanning | Uitvoeren onderhoud schip | Het uitvoeren van technisch onderhoud aan het schip. |
| | | Zorgdragen voor uitrusting | Het controleren en zonodig vervangen, repareren van de uitrusting aan boord van het schip. |
| | | Bewaken conditie lading / passagiers | Het tijdens de reis zorgdragen voor de veiligheid van de lading en passagiers op het schip. |
| 7 | Handhaver | Advies | Het geven van voorlichting, zowel publiek als individueel gericht, over wettelijke regelingen en handhaving. |
| | | Planning | Vergaren van vervoersmanagement en reisplanninginformatie, doen van risicoanalyses en plannen van inspecties. |
| | | Handhaving voortraject | Uitvoeren preventieve inspecties op schip, lading en bemanning. |
| | | Handhaving varen | Repressieve inspectie uitvoeren, bestaande uit houden van toezicht en verrichten van opsporingen. |
| | | Calamiteitenbestrijding | Het pro-actief, preventief en repressief bestrijden van calamiteiten en het verlenen van nazorg in geval een calamiteit optreedt. |
| 8 | Faciliterende en bevoorradende dienst | Bestellen/boeken | Het ontvangen en verwerken van bestellingen van derden om gebruik te maken van facilitaire diensten. |
| | | Plannen/reserveren | Het bestellen en boeken van faciliteiten om het schip van proviand, brandstof en reparaties te voorzien. |
| | | Uitvoeren | Het laden van proviand, brandstof en uitvoeren van reparaties voor het vertrek van het schip. |
| 9 | Stuwadoor | Capaciteitsplanning kade / kraan / automatisch geleide voertuigen | Tactische planning waarbij de beschikbare capaciteit van de kade, kranen en agv's wordt toebedeeld aan aankomende schepen. |
| | | Capaciteitsplanning stack | Tactische planning waarbij de beschikbare capaciteit van de stack wordt toebedeeld aan aankomende schepen. |
| | | Capaciteitsplanning docks | Tactische planning waarbij de beschikbare capaciteit van de docks wordt toebedeeld aan aankomende schepen. |
| | | Stack planning | De operationele planning van de stack (waar komt container X te staan?) |
| | | Schip/kadeplek/kraan toewijzing | Toewijzing van een kade en kraan aan een aankomend schip. |
| | | Operationele aansturing kraan / box / automatisch geleide voertuigen | De aansturing en uitvoering van het overslagproces. |
| | | Identificatie van container op schip | Identificatie van de container opdat deze op de juiste plek kan worden gelost. |

| | Rol | Taak | Omschrijving |
|---|---|---|---|
| | | Identificatie van container in de stack | Identificatie van de container opdat deze op de juiste plek kan worden geladen. |
| | | Identificatie van container/truck | Identificatie van de container opdat deze op de juiste plek kan worden opgeslagen op de terminal. |
| | | Calamiteitenbestrijding | Het pro-actief, preventief en repressief bestrijden van calamiteiten en het verlenen van nazorg in geval een calamiteit optreedt. |
| 10 | Navigerende schipper | Operationele melding | Het geven van een aankomstmelding aan de verkeersbegeleider bij nadering van een haven, sluis, brug of verkeerspost |
| | | Sluispassage | Het passeren van een sluis |
| | | Brugpassage | Het passeren van een brug |
| | | Terminal 'passage' | Het aanleggen en vertrekken aan/van de kade bij een terminal. |
| | | Navigeren | Het besturen van het schip. |
| | | Calamiteitenbestrijding | Het pro-actief, preventief en repressief bestrijden van calamiteiten en het verlenen van nazorg in geval een calamiteit optreedt. |
| 11 | Waterbeheerder | Nautische informatievoorziening | Het ontvangen, verwerken en ter beschikking stellen van informatie aan verkeersdeelnemers en andere derden omtrent de waterhuishouding. |
| | | Waterkwaliteit en waterhuishouding | Het monitoren, plannen en uitvoeren van activiteiten om de waterkwaliteit en het waterpeil te handhaven resp. te regelen. |
| 12 | Vaarwegbeheerder | Nautische informatievoorziening | Het ontvangen, verwerken en ter beschikking stellen van informatie aan verkeersdeelnemers en andere derden omtrent de verkeerssituatie en toestand van een vaarweg. |
| | | Investering | Het doen van investeringen teneinde de kwaliteit van de vaarweg te handhaven of verbeteren. |
| | | Innen vaargelden | Het innen van gelden bij gebruikers van de vaarweg. |
| | | Toestand vaarweg monitoren | Monitoren en controleren van de staat van de vaarweg. |
| | | Calamiteitenbestrijding | Het pro-actief, preventief en repressief bestrijden van calamiteiten en het verlenen van nazorg in geval een calamiteit optreedt. |
| 13 | Havenbeheerder | Nautische informatievoorziening | Het ontvangen, verwerken en ter beschikking stellen van informatie aan verkeersdeelnemers omtrent de verkeerssituatie en faciliteiten in de haven. |
| | | Investering | Het doen van investeringen teneinde de kwaliteit van de haven te handhaven of verbeteren. |
| | | Innen havengelden | Het innen van gelden bij gebruikers van de haven. |
| | | Toestand droge deel monitoren | Verwerken van meldingen, controleren en beheren ligplaatsen, overslag van gevaarlijke stoffen, controle van milieuwetten. |
| | | Toestand natte deel monitoren | Verwerken meldingen, overslag van gevaarlijke stoffen, controle milieuwetten (water) |

| | Rol | Taak | Omschrijving |
|---|---|---|---|
| | | Calamiteitenbestrijding | Het pro-actief, preventief en repressief bestrijden van calamiteiten en het verlenen van nazorg in geval een calamiteit optreedt. |
| 14 | Vlootbeheerder | Economische levensduur | Het vaststellen van de economische levensduur van de vloot en op basis daarvan beslissingen nemen ten aanzien van investeringen in de vloot. |
| | | Technische levensduur | Het vaststellen van de technische levensduur van de vloot en op basis daarvan beslissingen nemen ten aanzien van investeringen in de vloot. |
| | | Bewaken werk- en leefcondities | Het bekijken en vastleggen van de omstandigheden op de schepen en bewaken dat de juiste werk- en leefcondities hierbij gewaarborgd zijn. |
| | | Bewaken conditie schip | Het bekijken en vastleggen wat de actuele staat van het schip is en zonodig onderhoud plegen. |
| | | Bewaken conditie uitrusting | Het bekijken en vastleggen wat de actuele staat van de uitrusting van het schip en zonodig onderhoud plegen of vervangende onderdelen aanschaffen. |
| | | Bewaken vloot | Het bekijken en vastleggen wat de actuele staat is van de gehele vloot. |
| 15 | Terminal-beheerder | Economische levensduur | Het vaststellen van de economische levensduur van de terminal en op basis daarvan beslissingen nemen ten aanzien van investeringen in de terminal. |
| | | Technische levensduur | Het vaststellen van de technische levensduur van de terminal en op basis daarvan beslissingen nemen ten aanzien van investeringen in de terminal. |
| | | Bewaken werk- en leefcondities | Het bekijken en vastleggen van de omstandigheden op de terminal en bewaken dat de juiste werk- en leefcondities hierbij gewaarborgd zijn. |
| | | Bewaken conditie materieel | Het bekijken en vastleggen wat de actuele staat van het materieel is en zonodig onderhoud plegen of vervangende onderdelen aanschaffen. |
| | | Bewaken conditie uitrusting | Het bekijken en vastleggen wat de actuele staat van de uitrusting van het schip en zonodig onderhoud plegen of vervangende onderdelen aanschaffen. |
| | | Calamiteitenbestrijding | Het pro-actief, preventief en repressief bestrijden van calamiteiten en het verlenen van nazorg in geval een calamiteit optreedt. |
| 16 | Bevoegde autoriteit | Nautische informatievoorziening | Het ontvangen, verwerken en ter beschikking stellen van informatie aan verkeersdeelnemers omtrent de verkeerssituatie en faciliteiten in de haven. |
| | | Uitvoeren betalingen | Het financieel afhandelen van de gebruikmaking van infrastructuur door verkeersdeelnemers |
| | | Administratieve afhandeling | Het registeren en controleren van gegevens omtrent verkeersafhandeling en facturering |
| | | Kadetoewijzing | Verwerken vooraanmelding schip en toekennen kade. |

| | Rol | Taak | Omschrijving |
|---|---|---|---|
| | | Aanwijzingen geven | Toestemming dan wel een verbod geven om in te varen en aanwijzingen te geven aan verkeersdeelnemers hieromtrent. |
| | | Ondersteunen bij Calamiteitenbestrijding | Het pro-actief, preventief en repressief bestrijden van calamiteiten en het verlenen van nazorg in geval een calamiteit optreedt. |
| 17 | Objectbedienaar (brug en tunnel) | Nautische informatievoorziening | Het ontvangen, verwerken en ter beschikking stellen van informatie aan verkeersdeelnemers omtrent de verkeerssituatie rondom een brug. |
| | | Overzicht water | Het bijhouden van de actuele en verwachte status en een historisch overzicht van het verkeer rond de brug |
| | | Overzicht weg en rail | Het bijhouden van de actuele en verwachte status en een historisch overzicht van het verkeer op de weg en op het spoor rond de brug. |
| | | Aankomst en vertrek schip | Vaststellen aankomstvolgorde. aanwijzen wachtplaats, aanwijzen opstelplaats, aangeven invaarvolgorde en aanwijzingen geven voor invaren, afmeren en uitvaren. |
| | | Scheepvaartbegeleiding rond brug en tunnel | Verwerken vooraanmelding schip en toekennen toerbeurt. |
| | | Verkeersbegeleiding rond brug en tunnel | Het plannen, regelen en aansturen van het wegverkeer en waterverkeer rondom een brug. |
| | | Bedienen beweegbare brug | Het openen en sluiten van de brug en slagbomen aan de wegzijde. |
| | | Ondersteunen bij calamiteitenbestrijding | Het pro-actief, preventief en repressief ondersteuning bieden bij bestrijding van calamiteiten en het verlenen van nazorg in geval een calamiteit optreedt. |
| 18 | Verkeersleider op verkeerspost | Nautische informatievoorziening | Het ontvangen, verwerken en ter beschikking stellen van informatie aan verkeersdeelnemers omtrent de verkeerssituatie en faciliteiten rondom de verkeerspost. |
| | | Overzicht over gebied | Het bijhouden van de actuele en verwachte status en een historisch overzicht van het verkeer in het gebied rondom de verkeerspost. |
| | | Aankomst en vertrek schip | Vaststellen aankomstvolgorde, aanwijzen opstelplaats, vaarroute en aanwijzingen geven voor eventueel afmeren en uitvaren. |
| | | Verkeersbegeleiding binnen VTS D. gebied | Verwerken vooraanmelding schip, plannen verkeersbegeleiding en informeren navigator. |
| | | Verkeersbegeleiding binnen VTS sector | Verwerken vooraanmelding schip, plannen verkeersbegeleiding en informeren navigator. |
| | | Ondersteunen bij calamiteitenbestrijding | Het pro-actief, preventief en repressief ondersteuning bieden bij de bestrijding van calamiteiten en het verlenen van nazorg in geval een calamiteit optreedt. |
| 19 | Sluismeester | Nautische informatievoorziening | Het ontvangen, verwerken en ter beschikking stellen van informatie aan verkeersdeelnemers omtrent de verkeerssituatie rond en binnen een sluis. |

| | Rol | Taak | Omschrijving |
|---|---|---|---|
| | | Overzicht over gebied | Het bijhouden van de actuele en verwachte status en een historisch overzicht van het verkeer rond en binnen het sluiscomplex. |
| | | Aankomst en vertrek schip | Vaststellen aankomstvolgorde, aanwijzen wachtplaats, aanwijzen opstelplaats, aangeven invaarvolgorde en aanwijzingen geven voor invaren, afmeren en uitvaren. |
| | | Verkeersbegeleiding rond en binnen sluiscomplex | Verwerken vooraanmelding schip en toekennen toerbeurt. |
| | | Schutten | Het door de sluis schutten van een schip. |
| | | Ondersteunen bij calamiteitenbestrijding | Het pro-actief, preventief en repressief ondersteuning bieden bij de bestrijding van calamiteiten en het verlenen van nazorg in geval een calamiteit optreedt. |