Complex 4/01

Emily M. Weitzenböck

LEGAL ISSUES OF MARITIME VIRTUAL ORGANISATIONS

Institutt for rettsinformatikk
Postboks 6706 St Olavs plass
0130 Oslo

Henvendelser om denne bok kan gjøres til:

Institutt for rettsinformatikk
Postboks 6706 St. Olavs plass
0130 Oslo
Tlf. 22 85 01 01
www. jus.uio.no/iri/

ISBN 82-7226-043-3
ISSN 0806-1912

Utgitt i samarbeid med Unipub Forlag
Trykk: GCSM AS
Omslagsdesign Kitty Ensby

To my parents, Thomas and Jane Camilleri

FOREWORD

Interest in virtual organisations, also known as virtual enterprises, has grown in the last few years and these terms have become buzz-words in the business and management field. However, discussion and research on the legal characteristics and the legal issues regarding virtual organisations are a rather recent development. Therefore, when, in 1998, I first heard of a project proposing to explore the feasibility and characteristics of virtual organisations in the maritime domain, I was very eager to carry out research on the legal issues surrounding virtual organisations (besides being also intrigued by the project's name, as any proper "hitchhiker" would be…).

This study is based on a report which was written in the framework of the aforementioned project – the MARVIN project (MARitime Virtual enterprise Network: EP 29049) – that was funded by the European Commission within the ESPRIT programme. I am grateful to the Commission for their financial assistance. Needless to say, this study does not represent the opinion of the European Commission, nor is the Commission responsible for any use that might be made of any information appearing in it. Participating in the MARVIN project has been a wonderful opportunity for me to work with and learn from people from other, non-legal, fields such as software engineering, naval architecture, and the maritime business and industry. I am grateful to my colleagues and friends in MARVIN, for sharing their knowledge and expertise on the technical and maritime domain. Besides the University of Oslo, the MARVIN consortium comprises Det Norske Veritas AS, Norway; Xantic, The Netherlands; Germanischer Lloyd AG, Germany; University of Saarland (Institute for Business Information Systems), Germany; Instituto Superior Técnico (Unit of Marine Technology and Engineering), Portugal; Marenostrum (Recruamento de tripulações e Gestão de navios Lda.), Portugal; Lisnave Estaleiros Navais SA, Portugal; University of Patras (Department of Merchanical Engineering and Aeronautics, Laboratory for Manufacturing Systems), Greece and Neorion New S.A. Syros Shipyards, Greece.

My thanks also go to all the people at the Norwegian Research Centre for Computers and Law (NRCCL), both research and academic staff, for their friendship. I am indebted to Prof. Jon Bing, for his support which led the University of Oslo to join the MARVIN project and for his enthusiasm for my research on virtual organisations. I am also grateful to Beate Jacobsen, who was projects co-ordinator at the NRCCL when I started my MARVIN research, for

her support. I also thank my fellow researcher at the NRCCL, Rolf Riisnæs, who has seen earlier drafts of my MARVIN report, for his invaluable comments and insights on these drafts.

Last, but certainly not least, I am indebted to my husband Jan R. Weitzenböck, for his unstinting support and encouragement throughout this time.

Oslo, September 2001

Emily M. Weitzenböck

CONTENTS

ABBREVIATIONS

AWES	Association of West European Shipbuilders
BIMCO	Baltic and International Maritime Council
EDI	Electronic Data Interchange
ER-Company	Emergency Response Company
ICT	Information and Communication Technology
LOF	Lloyd's Standard Form of Salvage Agreement
MARAD form	the shipbuilding contract of the Maritime Subsidy Board of the US Department of Commerce Maritime Administration
MEIT	Maritime Enterprise Integration Tool
SAJ form	Shipbuilding Contract of the Shipowners Association of Japan
UNCITRAL	United Nations Commission on International Trade Law
UNIDROIT	International Institute for the Unification of Private Law

1. INTRODUCTION

As co-operation between enterprises, facilitated by developments in information and communications technology, becomes increasingly important in today's complex and borderless world, new forms of entrepreneurial co-operation are developing, such as virtual enterprises, also known as virtual organisations.

The shipping industry, like other industries, has recognised the importance of information technology - not least the Internet - as a business and communications tool. The growth of electronic commerce has also brought about a need to define and address the legal issues that arise when conducting one's business electronically. Awareness of such issues is important because it helps a business to secure a better business position, comply with regulatory obligations, and safeguard its rights.

This study is based on a report[1] compiled in the framework of the MARVIN project (MARitime VIrtual enterprise Network – No. EP 29049), funded by the European Commission within the ESPRIT programme. This project was set up to demonstrate an ICT-based[2] solution for improving emergency repair and planned maintenance processes in the maritime industry with the ultimate goal to cut down docking time, improve safety at sea and reduce impacts on the environment. One of the main objectives of this project is the development of a prototype software - the Maritime Enterprise Integration Tool (hereinafter referred to as the "MEIT") - to model, facilitate and co-ordinate the interaction between maritime companies forming a virtual organisation on the Internet.[3]

This study deals with Task 1.4 of the project, the objective of which was to establish a legal framework, in the interest of both clients (i.e. the shipowner or ship manager) and the partners who will supply services to them (e.g. shipyards, salvage companies, classification society, etc.),[4] for operating a virtual maritime organisation. A copy of the terms of reference of this task may be found in Appendix 1.

---

1. Weitzenböck, E., *Final legal framework for the maritime virtual organisation*, MARVIN Deliverable No. T1.4D2, November 2000.
2. Information and Communications Technology.
3. See MARVIN Project Summary at http://research.dnv.com/marvin/summary.html, last visited 31.08.2001.
4. The clients and service offerors or suppliers are hereinafter collectively referred to as the "users".

The focus of this study are the legal issues that arise from the creation and operation via the Internet of a virtual enterprise in the maritime domain. Other maritime law issues that may arise but which are not a consequence of the establishment of the virtual enterprise (e.g. the consequences of oil pollution and damage, or of collision, or of injury or loss of life), fall outside the scope of this analysis.

This study will commence with an analysis of the legal nature of the virtual organisation, with a look at the possible legal and business structures that may be used for such organisations (Chapter 2). This is then followed by a look at different aspects and features of the integration tool, and the relationship between the users themselves upon the creation of a virtual organisation.

Chapter 3 looks at the legal issues arising from the use of the integration tool by the users for the transmission of information, and at the protection of information and immaterial rights. A major concern of any potential user of the tool is that the system should be secure. Certain ship designs and data - information, which could be required by a yard that was contracted to repair a ship following a casualty - are very often protected from disclosure to third parties by confidentiality clauses. An analysis is made of this duty of confidentiality and of the rules of procedure developed by classification societies for the disclosure of such information, as well as its effect on the operation of the virtual organisation. Security concerns and the importance of safeguarding the confidentiality, integrity and authenticity of electronic messages, both in the design and in the subsequent use of the integration tool, are highlighted. This is followed by a brief study of the legality of use of encryption and digital signature technology for message transfer.

There is then an examination of the legal issues arising from the use of the integration tool and of the relationship between the user and the tool. Chapter 4 focuses on the functioning (or malfunctioning) of the integration tool itself and proposes the use of a framework agreement - the MEIT User Agreement - to deal *inter alia* with issues such as the formation and validity of electronic contracts, the extent to which such contracts are admissible as evidence, liability for defects in the integration tool and possible limitation thereof, choice of law clauses, choice of jurisdiction, and electronic data interchange ("EDI") issues such as message acknowledgement and contract formation. Some sample or draft clauses for such a MEIT User Agreement are proposed in Appendix 4.

Chapter 5 looks at the relationship between the users of the tool themselves and at the formation of contracts between such parties. Once a party has been selected to provide a required service (e.g. towage, salvage, etc.), the client and

the service provider will usually enter into a contractual relationship for the provision of such service. In the maritime field, one often finds a number of standard maritime contracts in use. This chapter will examine the contract formation stage relating to these special maritime contracts in the light of the proposed tool.

Input for this study was been obtained from a number of other research studies undertaken in the framework of the MARVIN project.[5] It should be mentioned that, in the MARVIN project, the focus was on issues that arise in two different business cases: emergency repair and planned maintenance of a vessel.[6]

Although the basis of this study are maritime virtual organisations, an attempt is made to also discuss general legal issues related to virtual organisations (such as their nature and characteristics, security aspects, etc.) which, it is hoped, will make this study of more general interest. The maritime virtual organisation may be taken as an illustration, as an example, of the use of virtual organisations in the business world.

5. In particular, Haenisch, J. (ed.), *Final user requirements and models* (business processes), MARVIN Deliverable No. T1.1D2, December 2000; Jaramillo, D. (ed.) , *Final user requirements and models (business information and product data)*, MARVIN Deliverable No. T1.2D2, January 2001; Angeli, R. (ed.)., *Final virtual organisation architecture*, MARVIN Deliverable No. T.1.3D2, November 2000; Angeli, R., Odendahl, C., Kraus, S., *Final specification of software and interfaces*, MARVIN Deliverable No. T3.1D2, (restricted), June 2000; and Makris S. (ed.), *Validation of Prototype*, MARVIN Deliverable T4.1D1, (restricted), June 2000.

6. In particular, the two business cases and the accompanying scenarios specified respectively in the Haenisch, J. (ed.)., *op. cit. supra* n. 5.

2. LEGAL NATURE OF THE VIRTUAL ORGANISATION

2.1 What is a virtual organisation?

Although the field of business management has recognised the growing importance of the virtual organisation in the business world, there is a dearth of legal literature on the legal nature and characteristics of the virtual organisation.

As Holland[7] states, there are a number of different terms to describe the phenomenon of novel forms of economic organisations such as virtual organisation, strategic web, network organisation and strategic/co-operative alliances. It is therefore important to clarify what is meant by the term "virtual organisation" or "virtual enterprise". Mertens & Faisst[8] define the virtual enterprise as:

> *"A virtual enterprise is a co-operation form of legally independent enterprises, institutions and/or individuals, that produce a service on the basis of a common business understanding. The co-operating units participate in the horizontal and/or the vertical collaboration with their core competencies and appear to third parties as a homogenous enterprise. Furthermore the institutionalisation of central management functions for design, management and development of the Virtual Enterprise are extensively abandoned and the necessary demand for co-ordination and harmonisation is covered by appropriate information and communication systems. The Virtual Enterprise is connected to a mission and ends with that mission."*[9]

---

7. Holland C.P., "The importance of Trust and Business Relationships in the Formation of Virtual Organisations", in *Organizational Virtualness: Proceedings of the VoNet Workshop, April 27-28, 1998,* 1998, Simowa Verlag Bern, p. 55.
8. Mertens, P., Faisst, W., "Virtuelle Unternehmen - Idee, Informationsverarbeitung, Illusion", in Scheer, A.-W., Organisationsstruckturen und Informationssysteme auf dem Prüfstand, 18. Saarbrücker Arbeitstagung 1997, Heidelberg 1997, pp. 101-135.
9. A comprehensive theoretical background of the concept of the virtual enterprise may be found in Odendahl, C and Scheer, A.-W., "The Concept of Virtual Enterprises and its Relevance for the Maritime Domain", in Guedes Soares, C., Brodda, J., (Eds.), Application of InformationTechnologies to the Maritime Industries, Edições Salamandra, Lisbon, 1999, pp. 11-31..

It is opportune to refer to the phases in the life-cycle of a virtual enterprise. Odendahl[10] lists the following:

(1) Identification of the need to co-operate, the definition of the goal to be reached by co-operation and the definition of the co-operation project;

(2) Partner Search: This process is a selection of the partner companies out of a pool of potential offerors for the different core competencies needed in the Virtual Enterprise.

(3) Contracting: Once the most suitable partners have been selected, the modalities of the co-operation should be determined through contracting between the partners.

(4) Operation: This is the performance of the co-operation.

(5) Dissolution of the Virtual Enterprise: This occurs once the task and goal of the Virtual Enterprise have been achieved.

2.2 Business structure of a virtual enterprise

A virtual enterprise, being a co-operation form of legally independent enterprises, may thus be formed among any of a number and mixture of the following business structures: sole traders, limited liability companies or other forms of partnerships or bodies of persons.

In fact, the virtual enterprise offers small and medium-sized enterprises (SMEs) the advantage of collaborating together by pooling their resources and core competencies, so as to be able to offer a common service to the customer that each of them individually would not otherwise have had the resources to offer. This is a major advantage for SMEs.

The question may be raised as to what kind of business structure does the virtual enterprise most resemble. In order to do this, one should first distinguish between two different types of virtual enterprise. On the one hand there may a stable virtual enterprise where there is one core partner which lays down the rules for collaboration and which outsources certain tasks to other independent enterprises (e.g. Dell company, Amazon.com). This has also been referred to as top-down virtualisation.[11] On the other hand, there may be dynamic networks consisting of individual independent enterprises which to-

10. *Ibid.*
11. See the discussion on the two directions of virtualisation in building a virtual enterprise in Odendahl, C and Scheer, A.-W., ibid.

gether embark on common action at the moment that a customer approaches them with an order or a problem. In the latter case, temporary collaboration results with shared leadership.[12] This has also been described as bottom-up virtualisation.[13]

2.2.1 Top-down virtualness

In this model of a virtual enterprise – also called planet-satellite organisations - there is high control by the core partner which outsources tasks to a number of legally independent units. One is likely to find that the core partner (planet) will enter into separate contracts with each of the smaller firms (satellites) to which it outsources tasks. Such contracts would lay down clear consequences (e.g. through the imposition of heavy penalties or agreement on pre-liquidated damages) for non-compliance by the small firm, since such non-compliance (e.g. delays in meeting deadlines, or refusal to perform) can have very serious consequences for the core partner. For example, because of non-performance of one enterprise, the other enterprises in the chain of production, as a consequence, will also end up being delayed. A delay might also mean that another enterprise, due to the delay, would be unable to perform its part in the chain of production because of temporary unavailable resources or manpower. Such contractual clauses are one way for the core partner to try to limit the risks that ensue from its dependency on the smaller enterprises.

2.2.2 Bottom up virtual enterprises

In this model of virtual enterprise, a number of economically and legally independent enterprises co-operate together to produce goods and/or services in a better way so as to be more competitive together in the market. Such co-operation forms may either be long-term oriented and based on the involvement of capital as well as contractual guarantees (these are sometimes also called strategic alliances or strategic networks) or else such co-operation forms may be short-term oriented, very flexible and dynamic (almost all definitions in literature on virtual enterprises refer to this latter form of organisation).

An important factor for business co-operation is trust. Trust plays an important role in both the strategic alliance and the virtual organisation. In strategic alliances trust is safeguarded through procedures and contracts.[14] An

12. See Jansen, W., Steenbakkers W. and Jägers, H. "Electronic Commerce and Virtual Organizations", in *Organizational Virtualness and Electronic Commerce: Proceedings of the 2nd International VoNet Workshop, September 23-24, 1999,* Simowa Verlag Bern, pp. 54-55.
13. See *supra* n. 9.

example of a strategic alliance is that between KLM and NorthWest Airlines which enhances the competitive position of the alliance participants in that the occupation level of the fleet increased due to combined flights and due to one of the participants being awarded landing rights as a license holder.[15]

As regards dynamic virtual enterprises, according to Jägers, Jansen and Steenbakkers[16], in contrast with strategic alliances and planet-satellite organisations, "the virtual organisation participants do not try to heighten this control through regulation or forms of control (using contracts for example) but rather through the pooling of knowledge and information." However, it is submitted that although there might not be a pre-existing contractual relationship between the independent enterprises forming a flexible and dynamic virtual enterprise (i.e. pre-existing the partner search prior to the creation of a virtual enterprise), once the partners have been identified there will be a need to establish a legal framework for the virtual organisation. This is also the view expressed by Odendahl, Reimer and Marzen[17] who explain that the concept of virtual enterprises is based on trust by definition and therefore it would initially appear that a legal framework does not have to be considered. However, these authors continue that the application of such a culture of trust in practice has proved to be a problem, and the culture of trust is opposed to the temporary character of a virtual enterprise because trust can only arise over a certain period of time.[18] Therefore, virtual enterprises depend on loose legal frameworks which may, for example, be implemented by electronic contracts.[19]

---

14. Jägers H, Jansen W., Steenbakkers W., "Characteristics of Virtual Organizations", in *Organizational Virtualness: Proceedings of the VoNet Workshop, April 27-28*, 1998, 1998, Simowa Verlag Bern, p. 73.
15. *Ibid, p. 68*.
16. *Ibid*.
17. Odendahl, C.; Reimer, S.; Marzen, S., "Fallstudie zum Projekt 'Konyeption und Entwicklung einer Kooperationsbörse zur kontinuierlichen Gestaltng Virtueller Unternehmen", Bibliothek der Kooperationsbörse, http://www.iwi.uni-sb.de/research/index_e.htm, last visited 31.08.2001.
18. A similar view is expressed by Pletsch, A. "Organizational Virtualness in Business and Legal Reality", in *Organizational Virtualness: Proceedings of the VoNet Workshop, April 27-28, 1998*, 1998, Simowa Verlag Bern, p. 86.
19. See Odendahl, C., Scheer, A.-W., supra n. 9.

Three different legal contracting methods are conceivable:[20]

1. each firm contracts separately with the customer;
2. the customer contracts with one main partner which, in turn, subcontracts to the other firms;
3. all individual members of the virtual enterprise jointly contract together with the customer.

The first option has the consequence that each enterprise would only be responsible for its individual part of the performance and cannot be called to account for another's delays or non-performance. If the customer wants to raise a claim for breach of warranty (e.g. defect) he would have to prove that a specific partner was responsible and sue only that partner. Furthermore, the customer is not assured that the whole product or service is performed completely, properly and on time. The risk of bad organisation and teamwork between the partner enterprises would be borne by the customer. This therefore does not appear suitable for application to virtual enterprise contracts.

The second option - that one partner would have primary responsibility, contract directly with the client and then sub-contract to the other partner firms - would have the advantage for the customer that it can sue that one primary partner for any contractual breach or non-performance. Consequently, the risk borne by the primary partner would be great, as it would be acting as a main contractor. Small enterprises do not usually have the capacity to assume such risks and therefore this type of contractual structure is not very suited for virtual enterprises which are generally made up of SMEs. This, however, is likely to be the typical contractual situation where there is a planet-satellite organisation, where the client enters into a contract (e.g. of sale or of services) with the primary firm (the planet) which, in turn, and very often unknown to the customer, sub-contracts parts of the operation to smaller firms which have high competency (the satellites).

The third option - where the individual partners in the virtual enterprise jointly contract with the customer - appears to be the contractual model most suited for a virtual enterprise. The contract would specify clearly the sharing of responsibility of all the service/product providers for the performance of the contract and the provision of the product or service to the customer. Each partner, in turn, could cover its liability by taking out appropriate insurance.

---

20. Berwanger, E., "The Legal Classification of Virtual Corporation According to German Law", in *Organizational Virtualness and Electronic Commerce: Proceedings of the 2nd International VoNet Workshop, September 23-24, 1999,* Simowa Verlag Bern, pp. 157-159.

The advantage for the customer is that he will not be dependent on just one partner and that partner's solvency for the performance of the contract.

The use of the term "virtual enterprise" might be rather misleading to someone, especially with a legal background, who is encountering this term for the first time, because it seems to give the impression that this is a new type of legal entity or legal person. However, from the above, it appears that one could use known and existing legal structures and mechanisms to regulate the operation of a virtual enterprise and the relationship between the members of the virtual enterprise and their customer. This can be either through the use of a contract[21] that resembles a consortium agreement to regulate the performance of the project, or, where necessary, through the formation of partnerships and associations which would have a separate legal personality. Where the virtual organisation has either just a contractual basis or is created merely on the basis of verbal agreement of the member partners, the virtual organisation would not constituted as a separate legal person.

2.3 The virtual enterprise created via the MEIT

2.3.1 The partner search task

Among the stages in the virtual enterprise life cycle, perhaps the most interesting is that of the partner search and identification. This task could be performed by an external third party – known as a business integrator - that is trusted by all the potential virtual enterprise partners. Such a business integrator would typically have management, technological and engineering competencies. Odendahl and Angeli describe how the partner search task could also be done by using the prototype system DEVICE of a co-operation exchange for Virtual Enterprises, which implements a five-layer filtering mechanism.[22] Each layer constitutes a specific pre-set criterion (e.g. price, competence, availability, etc.) on the basis of which the potential offerors will be selected or "filtered". In the MEIT prototype being developed in the MARVIN project, web-based agents will support the partner search, setting up and operation of the virtual enterprise in the two business cases selected, that is, emergency repair and routine maintenance of a vessel.

21. This is the case where all the individual members of the virtual enterprise jointly contract with the customer as abovementioned in alternative 3.
22. Odendahl, C.; Scheer, A.W, *op. cit.*, *supra* n. 9.

In the MARVIN project, the MEIT will facilitate and co-ordinate the interaction and co-operation of companies building up a virtual organisation to carry out the mission of repairing a ship in the shortest possible time. The MEIT is designed as a multi-agent system where every actor of the scenario, i.e. both partner companies comprising the virtual enterprise (e.g. shipyard (SY), emergency response company (ER), tug company (TC), salvage company (SA), classification society (CS)), as well as the customer (i.e. ship manger (SM), shipowner (SO)), is represented by its own agent (cf. Figure 1). An agent – an autonomous computational element which exists in the Internet and which contacts other elements of the Internet – represents the interests and goals of the relevant participant of the virtual enterprise. Through the use of agent technology, the communication between the customer and the virtual enterprise will be partly automated. Every agent representing a special actor of the scenario operates as an expert system (having its own knowledge base of rules) with the goal to satisfy the needs of the enterprise it forms parts of and the customer respectively.[23]

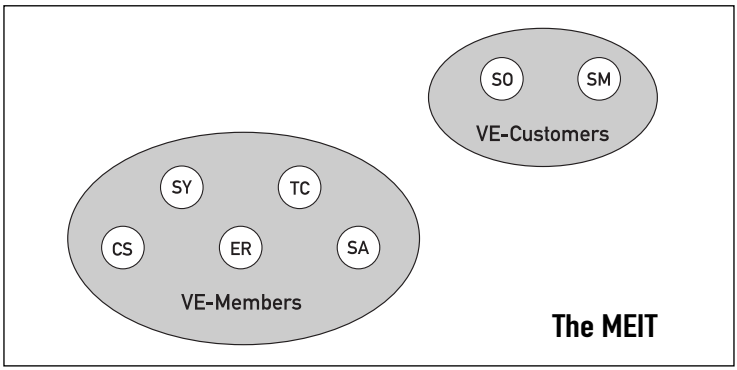


Figure 1: Some users of the MEIT

One could thus say that the MEIT, being a maritime enterprise integration tool, and as its name implies, is performing many of the functions that the business integrator in a virtual enterprise performs. However, there will still be a role for such a business integrator to act as a maritime services pro-

23. *Ibid*.

vider[24] to administer the MEIT system and perhaps to offer added services to the users of the tool (being both potential virtual enterprise members and its customers).

2.3.2 Web-based contract in MARVIN

A variant of the third contractual model outlined in Section 2.2.2 in the form of an electronic contract is being proposed for the maritime virtual enterprise created via the MEIT. This is because of some domain-specific peculiarities. In the MEIT, the partner search is limited by some characteristics of the maritime domain. For instance, the classification society is pre-defined by the shipowner at the time when the ship is constructed (although this may later on be changed). Therefore there would already be a pre-existing contractual relation with a specific classification society. Similarly, the Emergency-Response Company ("ER-Company") is usually pre-defined by the shipowner at the time the ship is acquired, because of the shipowner's obligation to comply with international maritime safety rules.[25] Nevertheless, since the tool will be used to send information to and to receive information from both the Classification Society and the ER-Company, such parties should agree on the validity of electronic communication through EDI contract-like clauses. This may be done by including such clauses in an agreement which all those who register with the MEIT, i.e. potential service offerors and customers should enter into. Such agreement – which in this study is called the MEIT User Agreement – should contain clauses on:

1. the use of the MEIT system by the users (i.e. those who register on the MEIT), and
2. the creation in future of a virtual enterprise by some of the users of the tool.

---

24. The role of such a maritime service provider is is examined in greater detail in Section 4.1 *infra*.
25. For example, the Oil Pollution Act of 1990 (OPA 90) requires that there should be shore based arrangements on a 24-hour basis for vessels carrying oil in bulk as cargo and operating in US waters, to enable rapid information to be obtained on salvage, damage stability and hull stress assessments. Moreover, within the Shipboard Oil Pollution Emergency Plan (SOPEP) according to MARPOL 73/78, Annex I, Chapter IV, Reg. 26, a contract address shall be nominated for competent casualty response and for stability/stress consideration. Furthermore, within the framework of SOLAS (Safety of Life at Sea), Chapter IX, for certain vessels the company should establish procedures to identify, describe and respond to potential emergency shipboard situations (the International Safety Management or ISM Code). An agreement for Emergency-Response Service with an ER-Company might be regarded as a valuable tool to fulfil such requirements.

The MEIT User Agreement will be dealt with in more detail in Chapter 4 where draft clauses for such an agreement are proposed.

However, there are other partners with whom there will be no pre-existing contractual relationship, e.g. tug company or shipyard to repair the vessel, and here the partner search and electronic contracting (phases 2 and 3 in the life-cycle of the virtual enterprise described in Section 2.1) become relevant. Of course, such actors would also have to register and enter into the MEIT User Agreement like all the other users. However, once such an actor, such as a shipyard, has been selected to carry out the repair the ship following an emergency or because of planned maintenance, there is a process of contract negotiation on the terms of the repair contract until agreement is reached and the repair contract signed. This matter is dealt with in further detail in Chapter 5.

3. SECURITY CONCERNS IN THE DESIGN AND USE OF THE INTEGRATION TOOL

3.1 Confidentiality of certain sensitive data

There are a number of instances where certain confidential or commercially sensitive data may be required to be transmitted via the integration tool. For example, when a company or organisation is registering with the MEIT system for the first time to offer its services or to be able to use the tool to obtain services, certain information considered by the applicant to be confidential information may be requested to be input into the tool.

Confidential information may also be required following the occurrence of an emergency. A particular feature of the maritime environment is that ships are mobile assets and emergencies may happen anywhere. Depending on the nature of the casualty, certain information regarding the ship may be required by a number of the parties involved in the casualty situation such as the ER-Company, the salvage company or the shipyard carrying out the repairs.

For example, in case of damage to the steel structure, the ER-Company may request additional information on the vessel such as steel drawings and results/data from previously performed strength analysis.[26] Moreover, when a salvage company is contracted and becomes part of the scenario, there is also a communication and information process between the ER-Company and the salvage company, in order to co-ordinate the salvage efforts. These processes may also involve the transfer of information, such as results of calculations and ship specific data.[27]

Very often, much of the information requested is protected by a contractual obligation of confidentiality (through a confidentiality clause or agreement) which restricts the disclosure to third parties of information such as a ship's plans, designs, technical descriptions/drawings and test data by the holder thereof (such as a classification society). Such clauses usually make it mandatory on the holder of the information to have or obtain the prior consent in writing of the owner of the particular document or information to disclose it to the third party requesting it. In addition, restrictions on, for example, the copying of such documents and information, may also follow from intellectual property law such as copyright law.

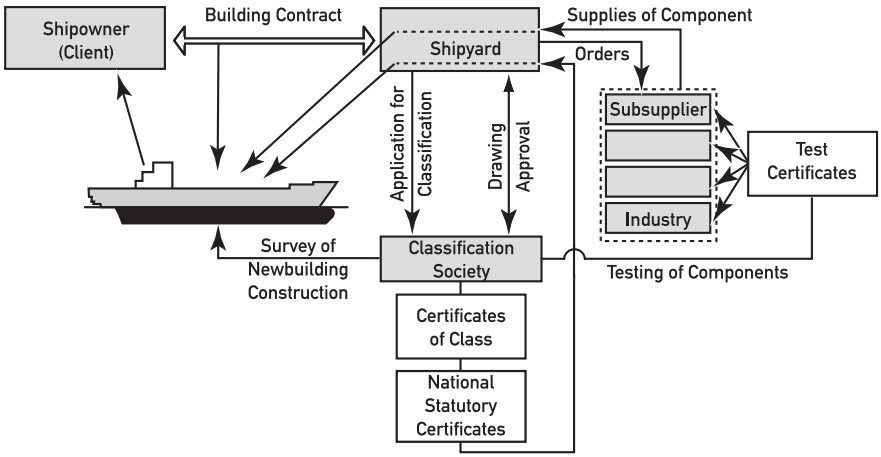
---

26. See the outline of such data requirements in Jaramillo, D. (ed.), *op. cit. supra* n. 5.
27. *Ibid.*

Some of the more common intellectual property clauses in standard shipbuilding contracts and some confidentiality clauses, which Classification Societies use in their standard agreements, are examined below. Then there is a study of some of the rules of practise which Classification Societies have developed for the disclosure of information, and this is followed by a look at what implications these may have on the virtual organisation.

3.1.1 Ownership of ship drawings and duty of confidentiality

Once a prospective shipowner has signed a shipbuilding contract with the shipyard of his choice, the shipowner usually enters into an agreement with a classification society for classification of the newbuilding of the ship. Figure 2 illustrates the complex relationships that come into play in the case of the newbuilding of a ship.



General Procedure for the Classification of Newbuilding of Ships

Figure 2: Newbuildings of Ships
(source: Germanischer Lloyd)

When the ship has been completed in accordance with the building contract between the shipowner and the shipyard,[28] and payment for the construction work has been made by the shipowner to the shipyard in terms of such con-

tract, the ownership of the ship is transferred to the shipowner.[29] However, it is extremely rare, as explained below, that the ownership of the ship designs, plans, information and documents related thereto are also transferred to the shipowner - in the vast majority of cases, it is the shipyard which built the ship which retains such intellectual property rights.

A newbuilding contract between the ship purchaser and the shipyard constructing the ship will frequently incorporate a clause stipulating that the shipbuilder is to retain title to all plans, drawings and other data relating to the design and construction of the ship.[30] This is the case for some of the standard shipbuilding contracts such as the Shipbuilding Contract of the Shipowners Association of Japan (the SAJ form) and that of the Association of West European Shipbuilders (the AWES form) which are widely used in the shipbuilding industry. Such a clause is often coupled with an express obligation upon the buyer not to divulge such information other than where required for the purposes of the ship's usual operation, repair and maintenance.

In fact, Article XVI (2) of the SAJ form provides that:

> *"The builder retains all rights with respect to the Specifications, and plans and working drawings, technical descriptions, calculations, test results and other data, information and documents concerning the design and construction of the vessel and the buyer undertakes therefore not to disclose the same or divulge any information contained therein to any third parties, without the prior written consent of the builder, excepting where it is necessary for usual operation, repair and maintenance of the vessel."*

The AWES form also provides that the ship builder retains all rights on the abovementioned documents (i.e. specification(s), general plans, working drawings, etc.) and that the purchaser undertakes not to bring them to the knowledge of third parties without the prior written consent of the ship builder. However, the AWES clause (Article 8(a)) continues that the showing of these plans and drawings shall not unreasonably be denied by the ship builder if it is necessary for carrying out repairs to the vessel. The implication

---

28. A common condition in such building agreements is that a classification certificate has been issued by the classification society in respect of such ship and that the necessary national statutory certificates have been obtained.
29. Where payment for the shipbuilding is done in instalments after each specific section of the ship has been constructed, title may pass before the completion of the vessel. See Goldrein, I. (ed.), *Ship sale and purchase*, 3rd ed., 1998, LLP, p. 32 and Curtis, S., *The Law of Shipbuilding Contracts*, 2nd ed., 1996, LLP p. 113.
30. See Curtis, S., *supra* n. 29, p. 207.

is that, under the AWES form, the ship builder's consent would have to be obtained even for the carrying out of repairs of the vessel.

The shipbuilding contract of the Maritime Subsidy Board of the US Department of Commerce Maritime Administration (the MARAD form) contains a detailed provision on the rights of the purchaser with respect to engineering and design data. The basic principle is that all plans and other specified design and engineering data required to be furnished to the purchaser by the plans and specifications and produced by the ship builder in the performance of the shipbuilding contract are deemed to be the sole property of the purchaser and the Maritime Board as their interests appear. This clause is reproduced in full in Appendix 2.

It therefore depends on the particular terms of the shipbuilding contract whether the builder has retained ownership of the ship's general drawings, technical descriptions and other ship information or whether these are the property of the shipowner.[31]

In the case of a newbuilding of a ship, following the building contract between the shipyard building the ship and the prospective shipowner, the shipyard enters into an agreement with a classification society for the classification of the newbuilding. The newbuilding agreement between the classification society and the shipyard usually contains a confidentiality clause, such as the following:

> *"(1) (a) All plans, drawings, specifications and information given to the classification soc iety in the performance of this agreement shall be treated as confidential by the classification society, and shall not be used for any other purpose than for which they have been furnished without prior written consent of the shipyard.*
>
> *(b) However, during the construction and fabrication of the vessel the classification society is entitled, but not obliged, to submit information concerning the classification of the vessel, at the discretion of the classification society, to the owner. Such information shall be given in writing with a copy to the shipyard."*[32]

---

31. Where, as is common, the newbuilding is to be constructed to a standard design which has been developed and marketed by the builder, he will obviously supply the initial draft of both the specifications and the principal plan and drawings but where the vessel is to be constructed to a non-standard design, the specifications may initially be prepared by either party. See Curtis, S., *The Law of Shipbuilding Contracts*, *supra* n. 29, p. 228.
32. This clause is based on the confidentiality clause in Det Norske Veritas' standard agreement for classification of a newbuilding.

When a ship has been registered with a classification society, a copy of the ship's documents such as the designs, drawings, specifications and surveys, is usually held by the classification society. In fact, in practice, especially where a ship has been owned by a number of successive owners, it is often the case that it is the classification society with which a ship is registered that holds the most complete set of the ship's documents.

It is common to find a confidentiality clause in the agreement with a classification society for the carrying out of the necessary classification and statutory surveys on a ship. One also comes across confidentiality clauses in other standard shipping agreements such as a classification of material and components agreement between the shipowner and the classification society, such as the following clause (reproduced from Det Norske Veritas' standard agreement for the performance of (classification) work):

"Confidentiality

(1) The Client and DNV [Det Norske Veritas] mutually agree that they will not disclose to third Parties without the prior written consent of the other Party, any information obtained from each other in connection with the performance of the work. However, each Party may give such information which is:
(a) known to the Party prior to obtaining it from the other Party
(b) part of the public domain at the time of disclosure
(c) required to be disclosed by official authorities in accordance with applicable law.
The Client and DNV may give information obtained from each other to their subcontractors to the extent necessary for the performance of the work without prior written consent, provided that written confidentiality agreements are secured from such subcontractors. Such confidentiality agreements shall be in terms substantially the same as in this article.

(2) The parties' obligations contained in this article shall continue notwithstanding the completion of the performance of the work or termination of the Agreement."

Some of the ship's documents may also be held by the ER-Company with which the ship is registered for emergency response services. Examples of such information are hull drawings (e.g. line drawings, computer model of hull surface). Such drawings are also normally held under strict obligations of confidentiality by the ER-Company.

3.1.2 Rules of practice of classification societies on disclosure of information

Because of the proprietary nature of some of the ship's documents, as well as because of their contractual duties to keep confidential the ship documents and information, classification societies seek to ensure that no unauthorised disclosure of the ship's documents is made. In fact, the internal regulations of Det Norske Veritas for disclosure of records state that:

> ***"B600 Disclosure of Information***
>
> ***601*** *The Society will not disclose any information received or reports made in connection with classification to any other than those entitled thereto ….. or those having been given the right to receive information by legislation, court decision or by written permission by the owner.*
>
> *The supply of information may take place electronically and on a continual basis, e.g. by on-line access to the Society's databases.*
>
> ***602*** *The Society will not disclose information which can be considered as the property of another party except when this party's permission is given in writing.*
>
> ***603*** *Internal communication, notes, calculations, etc. produced within the Society in connection with classification will not be disclosed to other parties.*
>
> ***604*** *Notwithstanding 601 to 603, authorised representatives of the National Maritime Authorities or of the audit team of IACS[33] performing Quality Audits, will upon request have access to such information. These representatives are to confirm in writing that they are not in any manner allowed to reproduce or communicate such information to other parties."*

A somewhat similar provision – though without the requirement that the consent should be in writing - is found in Germanischer Lloyd's "General Terms and Conditions", viz.

> ***"D. Confidentiality***
>
> *GL [Germanisher Lloyd] maintains confidentiality with respect to all documents and other kinds of information received in connection with the orders entrusted to the Society. Documents and information can only be made available to third parties with the approval of the person authorised to permit such disclosure. However, this shall not apply to the obligations GL has towards the administrations of flag states."*[34]

33. International Association of Classification Societies.

Thus the general rule is that disclosure of ship information and/or documents to third parties is made only to those persons who have been given the right to receive such information by the owner of such information (whoever this owner may be, i.e. the shipyard that built the ship, the shipowner, etc.). Figure 3 provides a quick guide of what kind of permission is required for the Classification Society to provide certain ship information depending on who is requesting the information.

Table B1 Disclosure of Information

Information in question	Owner	Flag State Authority	Port State Authority	Insurance Company*	Yard
Newbuildings: Approved "as carried out drawings"	2)	1)			4)
Ships in Operation: a) Class and statutory certificates issued by the Society, dates of surveys, dates and text of Conditions of Class or Recommendations given b) Survey Reports	4) 4) + 1)	1) 1)	1) 2)	1)** 3)	
Other Information: Correspondence with yard or owner	2)	2)		2)	2)

1) Upon request
2) When accepted by owner or ship yard or copyright holder as applicable
3) When accepted by owner or through special clause in insurance contract
4) Automatically available

* Insurance company means P&I Club and Hull & Machinery Underwriters
** Overdue Conditions of Class, Recommendations only

Figure 3: Disclosure of Information
(source: Det Norske Veritas)

34. Section 1, paragraph D, Germanischer Lloyd's "General Terms and Conditions", 2001 Edition, available at http://www.germanlloyd.org/member/conditions/conditions_gl.pdf, last visited 31.08.2001.

3.1.3 Effect of this on the virtual organisation

In practise, the consent in writing from the owner of the documentation for the release of the ship documentation to a third party requesting such documentation, is sent to the classification society in question via fax (which may be confirmed by the sending of the original hardcopy by mail).

Where the requirement for the consent of the owner of the documentation is interpreted by the classification society to mean that it must be obtained in writing on paper (e.g. sent through facsimile or in hardcopy through the post), a problem arises for the electronic transmission of such consent via the MEIT tool. In such a case, there is need for a change in the perspective and interpretation by the classification society in the sense that an electronic message such as an e-mail could still be considered to be a writing since it contains many of the essential characteristics of a writing, i.e. the message content is unalterable, it may be stored and viewed several times (i.e. it is not ephemeral in nature) and in this sense is permanent. The main reason for such an approach by classification societies seems to be the fact that classification societies want to ensure that the consent is really coming from the owner of the documents and not by someone else purporting to be him/her. Therefore great importance is attached to the logo of the shipowner or shipyard appearing on the face of the fax or hardcopy letter. However, it is submitted that similar – if not better – reassurance[35] of the authenticity and integrity of the message could be given by encrypting and digitally signing such messages.[36] It should be mentioned that the requirement for the consent to be "in writing" that existed in Germanischer Lloyd's rule prior to 2001[37] was removed – a step that facilitates the interpretation and application of this rule to admit electronic transmission of consent.

A clause could still, however, be inserted in the terms and conditions of the MEIT User Agreement which states that where any action is required by any users of the MEIT to be carried out in writing or by using a paper document, that requirement is met if the action is carried out by using one or more data messages.[38] In addition, if one wants to ensure message integrity, this clause

35. A logo on a fax message, especially in view of the sometimes poor resolution of facsimile machines, may easily be forged.
36. See *infra*. Section 3.2.
37. The previous version read as follows:
"Germanisher Lloyd will treat as confidential any documentation and information received in connection with orders placed with the Society. Such documentation and information may be passed on to third parties solely with prior written consent of the party entitled thereto. Proof of the power of disposal is to be furnished from case to case.
The above is without prejudice to any obligations towards the authorities of the state of the flag."

could perhaps also be qualified that such interpretation applies where the data message is sent in a secure format, e.g. encrypted. This clause would apply if the owner of the information/document is a user of the MEIT and hence a party to the MEIT User Agreement but if the owner is not a MEIT system user, he/she would not be bound by the terms and conditions of the MEIT User Agreement.[39] Therefore, much depends on how the requirement of writing in such clauses is interpreted by the classification society to whom the request for the documents was addressed.

3.2 Security Issues: Encryption and Digital Signatures

3.2.1 Introduction

Any business needs to maintain a degree of security over its information be it client information, intellectual property-protected information or confidential information. Where such a business uses electronic means of data storage and has connections to the outside world via the Internet, the risks of external attack (e.g. through hacking or a virus) increase. Moreover, because of the relative anonymity that an Internet user to a certain extent has, concerns over the identity of the sender of the message and of the integrity of the message also arise. It is therefore essential that the MEIT system that is being developed[40] guarantees both confidentiality of the contents of the message sent as well as message integrity and authenticity (in the sense that the message which the recipient receives is identical to that transmitted by the sender and is indeed that transmitted by the sender).

A number of security concerns were addressed in the architecture of the MEIT itself.[41] The MEIT architecture will have both the data management as well as the reasoning component of the agents running on the MEIT server. This increases the security of the system since as little data as possible is exchanged over the network, and therefore the risks of commercially sensitive

38. See draft clause 11 in Appendix 4. This proposed clause is based on Article 17 of the UNCITRAL Model Law on Electronic Commerce of 1996, available at http://www.jus.uio.no/lm/un.electronic.commerce.model.law.1996/doc.html, last visited 31.08.2001.
39. Where the owner of the information/document is not a user of the MEIT, a proposed solution could be that the shipowner requesting the disclosure of information would give a form of guarantee to the classification society to cover any eventual economic responsibility of the latter following the disclosure of such information/document.
40. At the time of writing, the MARVIN prototype is still being developed.
41. See, in particular, Angeli, R., Odendahl, C., Kraus, S, *op. cit. supra n.* 5.

data being intercepted while flowing over the network are kept at a low. It is also planned to have defined read/write rights for every firm in the virtual enterprise according to its company type and involvement in a certain process. The agents will control these rights and permit or deny respectively access to certain data. Thus, access to the related data is directly granted by the agent who is the owner of the relevant data and the interface to work with the data is maintained by the same agent.[42]

However, although as illustrated above, a number of security concerns have already been addressed in the very architecture of the MEIT, the MEIT tool could be made even more secure by taking further measures to ensure that the data objects transmitted via the MEIT are not intercepted, spied on or, worse still, tampered with (i.e. altered) or destroyed. Such security concerns may be addressed by the use of encryption and digital signature technology.

Although it has been decided[43] that encryption will not be implemented in the MEIT prototype, encryption is a feature that can be implemented without much difficulty in a commercial version of the tool.[44] For example, Java 2 (v1.2), provides different interfaces to encode data objects using strong data encryption algorithms, which have been extended in a recently released Java 2 (v1.3). Since the agents in the MEIT are implemented in Java, it should not be difficult to implement the strong data encryption algorithms that are provided by Java. For example, the package "javax.crypto" of JDK 1.2 provides both algorithms for asymmetric key and symmetric key encryption.

Although encryption will not be implemented in the MEIT prototype, it is still considered useful to look at some of the legal issues that can arise from the implementation and use of such technology. It is not proposed to enter into too much technical details since the technology changes very fast and encryption software is continually being developed to support higher levels of security. However, before looking at the broad legal issues that may arise, there is a brief introduction to encryption and digital signature technology.

---

42. This technical information on the security aspects of the MEIT is based on the MARVIN Deliverable T3.1D2, Angeli, R., Odendahl, C., Kraus, supra n. 5, at Section 2.2.2, pp. 37-38.
43. *Ibid.*
44. Technical details on how this could be implemented may also be found in another (technical) document in MARVIN, *ibid.*

3.2.2 What are encryption and digital signatures?

Encryption is a widely used method to ensure the privacy and security of electronic communication. There are two common forms of cryptography in widespread use:

(i) private key encryption (symmetric encryption): Both parties (sender and receiver) use the same key. The disadvantages of this is that it is necessary for both parties to know and agree the key in advance and to keep it completely secret thereafter. There is need for a key exchange mechanism before the encrypted transmissions can start, and two possible attack points for any third party trying to obtain the key.[45]

(ii) public key encryption (asymmetric encryption): Each party has two keys: a public key which can be published to the world at large and a private key which must be kept secret. There is no need for one party to an exchange to know the other party's private key; it is sufficient that he/she knows the other person's public key. The sender encrypts the message with the recipient's public key and the recipient can decrypt and read the message with his own private key. No one other than the intended recipient would be able to decrypt and read the original message.[46]

Thus one of the main concerns mentioned above, i.e. confidentiality of the message being transmitted, is addressed by encryption. Cryptography can also be used to ensure message authenticity and data integrity, an essential function for the MEIT tool. This may be done through the use of a digital signature using public key cryptography. Such a digital signature has two features which are similar to those of a hand-written signature: it is unique to the subscriber and it is different every time. The signature is calculated as follows. As public key cryptography is computationally very demanding, it takes too long to sign (i.e. encrypt) large documents. Instead, a special hash function or algorithm, used to reduce the amount of information that must be encrypted and decrypted, is applied to the message and produces a condensed message digest that is unique for each message. The sender encrypts the message digest using

---

45. Brazell, L., "Encryption Security: Encryption in the Real World", [1999] *European Intellectual Property Review 17*.

46. Public key encryption is a lot heavier on computing power than private key and so sometimes a "combination" of both is used. The recipient's public key is used only to encrypt a session key. The plaintext of the message is encrypted with the session key. Both message and session key are then sent to the recipient, who decrypts the session key using their private key and can then decrypt the message. This mixed method is known as a digital envelope, where the public key encryption of the session key acts as an envelope for the private key encrypted message. See Brazell, L., *supra* n. 45, p. 19.

his/her private key and sends the original text and the encrypted message digest to the intended recipient. To verify the sender's signature and ensure the integrity of the message received, the recipient (i) applies the same hash algorithm to the original message text and generates a message digest and (ii) decrypts the sender's message digest using the sender's public key. If the decrypted digest matches the recipient's digest, the integrity and authenticity of the message can be established.

A digital signature does not, as such, *per se* make any contribution to the confidentiality of the message since the message may be transmitted in plain text, with only the message digest encrypted to give the signature.[47]

However, applying the sender's public key is not enough to ensure that a digitally signed document came from a particular individual. The recipient must also have confidence that the private-public key used to sign/verify the document belongs to the sender and that the sender alone possessed the private key, particularly when there is no pre-existing relationship between the sender and the recipient. One method developed to ensure the recipient of a digital signature that he/she can trust that the signature came from a particular individual, is digital public key certification.[48] The idea is that a person (the key holder) first needs to provide sufficient evidence to a certification authority as to his/her identity and, once satisfied, the certification authority would then certify the relation between the identity concerned with the relevant key, by issuing a digital certificate.

A digital certificate therefore serves as a source of trust. It indicates that a trusted entity[49] vouches for the link between an individual and his public key. A digital certificate is an electronic document, digitally signed by some trusted entity, that contains information about an individual, including the individual's public key. In practice, the system works as follows. When an individual digitally signs a document, he simply attaches a copy of his digital certificate issued by the trusted entity. When the recipient receives the message and the accompanying digital certificate, he can rely on the public key of the trusted third party that issued the digital certificate to authenticate the message. Thus, a message recipient can now link a particular message to a particular person,

47. For better security one should have two pairs of keys, one to produce the signature and another to encrypt the session key.
48. See Baker, S. A. & Hurst, P. R., *The Limits of Trust: Cryptography, Governments, and Electronic Commerce*, 1998, Kluwer Law International, p. 251.
49. Such an entity is sometimes referred to as a Certification Service Provider or Certification Authority.

instead of simply linking the message to a particular public key.[50] In a certification system, there will be need for a repository which will contain important information on the certificates, such as for example, the date of revocation of a particular certificate.

A further possible function of digital signatures is to establish the time of creation of a message or document, if a time-stamp is included in the text, as this would also be unalterable without changing the message digest.[51] Time-stamping is often also rendered as a separate service.[52]

3.2.3 Encryption Regulation

Cryptography may therefore address both issues of confidentiality (through the use of encryption technology) as well as message authenticity and data integrity (through the use of digital signatures using public key cryptography). Although encryption will not be a feature of the MEIT prototype, as explained above,[53] it may and, it is submitted, should be added on at a later stage during the development of a commercial version of the tool.

However, the problem that next arises is whether the use of encryption technology is permitted and legal. Historically, governments have considered encryption technologies as "dual use goods" in that they may be used both for a civil as well as a military purpose. However, national laws vary in their treatment of cryptographic equipment and software and the domestic sale, possession, use and importation thereof as well as the export of such products may be subject to controls and restrictions under national law, European Community ("EC") law and in terms of the state's international obligations.

3.2.3.1 Controls on exports

3.2.3.1.1 International rules on encryption: the Wassenaar Arrangement

The Wassenaar Arrangement,[54] which came into effect on July 12, 1996, is an agreement between thirty-three countries[55] on Export Controls for Conventional Arms and Dual-Use Goods and Technologies. Germany, Greece, The

50. Baker, S. A., *supra* n. 48, p. 252.
51. Brazell, L., *supra* n. 45, p. 22.
52. Such a service is usually provided by a time stamping authority that would certify that a particular message with a particular signature exists at a defined time.
53. See Section 3.2.1 above.
54. For more information see the Wassenaar Arrangement web site at http://www.wassenaar.org, last visited 31.08.2001.

Netherlands, Norway and Portugal – the countries where the MARVIN partners are based - are all members of the Wassenaar Arrangement.

Cryptography is controlled as "information security" and is designated as a sensitive dual-use item under Category 5 Part 2 of the dual-use list. The participating states agreed to treat with vigilance those items on the lists of dual-use goods and to control these items with the objective of preventing unauthorised transfers or re-transfers of these items to non-participating states.[56] Transfers may be authorised according to a state's own policies and discretion.

In their plenary meeting of December 2 and 3, 1998, the Wassenaar member states agreed on new export control rules for encryption techniques. Export controls were relaxed and it was provided that in the future, products with a symmetric algorithm will only be subject to export controls if they have a key length in excess of 56 bits.[57] As regards products with an asymmetric algorithm,[58] these are controlled where the security of the algorithm is based on any of the following:

1. Factorisation of integers in excess of 512 bits (e.g. RSA);
2. Computation of discrete logarithms in a multiplicative group of a finite field of size greater than 512 bits;
3. Discrete logarithms in a group other than mentioned in 5.A.2.a.1.b.2 in excess of 112 bits.

It should be pointed out that, up to and until November 2000, mass market products which satisfied the following conditions[59] were subject to export controls only with key length exceeding 64 bits:

a. Generally available to the public by being sold, without restriction, from stock at retail selling points by means of any of the following:

---

55. The participating states of the Wassenaar Arrangement are: Argentina, Australia, Austria, Belgium, Bulgaria, Canada, Czech Republic, Denmark, Finland, France, Germany, Greece, Hungary, Ireland, Italy, Japan, Luxembourg, Netherlands, New Zealand, Norway, Poland, the Republic of Korea, Portugal, Romania, Russian Federation, Slovakia, Spain, Sweden, Switzerland, Turkey, Ukraine, United Kingdom, and the United States.
56. See Wassenaar Arrangement, §II.4.
57. See Wassenaar Arrangement Dual-Use List, Category 5 Part 2, No. 5.A.2.a.1.a, version as at 01.12.2000.
58. See Wassenaar Arrangement Dual-Use List, Category 5 Part 2, No. 5.A.2.a.1.b.
59. These are the conditions in the Cryptography Note inserted in Category 5 Part 2 during the December 2, 1998 revision of Wassanaar and recently revised in the December 1, 2000 revision of Wassenaar. This revision has been transposed also in Annex 1 of Regulation 1334/2000 of the European Union – see Section 3.2.3.1.2 *infra*.

i. over-the-counter transactions;

ii. mail order transactions;

iii. electronic transactions: or

iv. telephone call transactions;

b. the cryptographic functionality cannot easily be changed by the user;

c. the products are designed for installation by the user without further substantial support by the supplier;

d. the product does not contain a symmetric algorithm employing a key length exceeding 64 bits; and

e. when necessary, details of the items are accessible and will be provided, upon request, to the appropriate authority in the exporter's country in order to ascertain compliance with conditions described in paragraphs a to d above.

However, the 64 bit limitation in paragraph (d) was removed at the last plenary meeting (i.e. the 6th Plenary) of the Wassenaar member states on December 1, 2000. This means that, today, all mass market products that satisfy the other abovementioned conditions of the Cryptography Note, are not subject to export controls, regardless of the key length.

The Wassenaar Arrangement is not an international treaty but is merely designed to allow the Participating States to exchange views and information on international trade in conventional arms and dual-use goods and technologies. Participating States commit to adjust their national export control policies to adhere to the Wassenaar Arrangement Control Lists, but this commitment is discretionary in nature and not mandatory.[60] In fact, a number of states have more stringent controls on encryption than those laid down in the Wassenaar Arrangement (e.g. Russia and China).

3.2.3.1.2 The situation in the European Union

Recent developments in the European Union ("EU") will facilitate the movement of dual-use goods, including cryptography, among Community states and between Community States and the following ten countries: Australia, Canada, the Czech Republic, Hungary, Japan, New Zealand, Norway, Poland, Switzerland and the U.S. A new Council Regulation No. 1334/2000

60. See the website of the Electronic Privacy Information Centre on Cryptography and Liberty 2000 which contains an international survey of encryption policies at the following URL address http://www.epic.org/crypto/intl/, last visited 31.08.2001.

setting up a Community regime for the control of exports of dual-use items and technology was published on June 30, 2000 (the "Dual-Use Regulation").[61] It entered into force on September 29, 2000 and replaced the earlier 1994 Council Regulation No. 3381/94[62]. As an EU Regulation[63], it is directly applicable in the territory of all the EU Member States, and constitutes direct legislation[64] by the Community.[65]

This Regulation has a list of controlled goods in its Annex I which is in line with that of the Wassenaar Arrangement. Controls do not apply to generally available software and public domain software and technology pursuant to the General Software Note and the General Technology Note, the text of which is reproduced in Appendix 3 below. Controls can still be imposed on goods which could be used in the development of weapons of mass destruction.[66] Following the abovementioned[67] relaxation of control parameters regarding mass market products at the December 1, 2000 Wassenaar Meeting, Regulation 458/2001[68] updated the Cryptography Note in Category 5 Part 2 goods in Annex 1 to remove the 64-bit key length restriction.

According to Regulation 1334/2000 (as amended):

(1) The transfer or movement of dual-use goods from one EU member state to another is entirely liberalised, with the exception of the following highly specialised products listed in Annex IV of the Regulation:[69]

---

61. O.J. L 159, 30.06.2000, pp. 0001-0215.
62. O.J. L 367, 31.12.1994, p. 1 – Regulation as amended by Regulation No. 837/95, O.J. L 90, 21.04.1995, pp. 0001-0007.
63. Article 189 of the Treaty of Rome provides that "A regulation shall have general application. It shall be binding in its entirety and directly applicable in all Member States."
64. As Wyatt & Dashwood explain, "Regulations, in short, are to be treated as "law" in every sense of the word. National courts must take judicial notice of them in their entirety; specific provisions contained therein may bestow on individuals rights as against other individuals or Member States; and their effect in a particular area may be to pre-empt national legislative competence.", Wyatt & Dashwood's *European Community Law*, 3rd ed., London, Sweet & Maxwell, 1993.
65. However, certain enforcement provisions in the Regulation, such as Article 19, would need to be implemented in each respective Member State.
66. Although this Dual-Use Regulation greatly liberalises export controls, the European Commission could still impose some restrictions on exports under a "catch-all" clause which would allow products to be controlled even if they were not on the list of controlled items, if such goods could be used in the development of weapons of mass destruction – see Article 4, Dual-Use Regulation.
67. See *supra* Section 3.2.3.1.1.
68. See Council Regulation (EC) No 458/2001 of 6 March 2001 amending Regulation (EC) No 1334/2000 with regard to the list of controlled dual-use items and technology when exported, O.J. L 065, 07/03/2001, pp. 0019-0019.

a. equipment designed or modified to perform cryptanalysis items,

b. software having the characteristics, or performing or simulating the functions of cryptanalytical equipment,

c. only technology for the development, production or use of the goods specified in (a) and (b) above.

An individual export authorisation is required for the specialised products in Annex IV abovementioned.

(2) Export of products falling within the list of controlled goods[70] from a Community Member State to Australia, Canada, the Czech Republic, Hungary, Japan, New Zealand, Norway, Poland, Switzerland or the U.S. requires a Community General Export Authorisation, which would be valid for export from all EU countries. The Community General Export Authorisation does not cover the specialised cryptanalysis products specified in (1) above, in which case an individual export authorisation should be sought.

(3) Exports of products falling within the list of controlled goods[71] from a Community Member State to countries other than those mentioned in (1) or (2) above require authorisation (through either a general authorisation[72] or an individual authorisation). Such a license would be valid for export to one particular country.

Another area where national laws could differ concerns what is called "intangible" technology relating to encryption. This would include transfers of technology through meetings, correspondence and nowadays, through electronic mail and the Internet.[73] The Wassenaar Arrangement[74] states that it is important to have comprehensive controls on listed software and technology, including controls on intangible transfers. Although it does not oblige member states to control "intangible" exports such as downloading encryption

69. See Article 21 (1) and Annex IV of Reg. 1334/2000, *supra* n. 61 at p. 7 and p. 208.
70. This list matches the list of controlled goods attached to the Wassenaar Arrangement. That is, export of products with a symmetric algorithm are subject to export controls if they have a key length in excess of 56 bits – see *supra* n. 57. Export of certain products with an asymmetric algorithm may also be subject to export authorisation – see *supra* n. 58. Mass market products which satisfy certain conditions are not subject to export controls – see *supra* n. 59.
71. See *supra* n. 70.
72. except for cryptanalysis products mentioned in (1) above which require an individual export authorisation – see Reg. 1334/2000, Article 6(3), 7(1).
73. See Baker, S. A., *supra* n. 48, p. 74.
74. See Statements of Understanding and Validity Notes of the Wassenaar Arrangement.

software off the Internet, it encourages countries which currently do not have legislation to permit control regarding intangible transfers to "consider whatever action is necessary to address this issue." However, the EU Regulation 1334/2000 now considers as an export the transmission of software or technology by electronic media, fax or telephone to a destination outside the Community. This includes the oral transmission of technology by telephone only where the technology is contained in a document the relevant part of which is read out over the telephone, or is described over the telephone in such a way as to achieve substantially the same result.[75]

3.2.3.1.3 Other countries

The Dual-Use Regulation is likely to trigger off similar relaxation of controls of dual-use goods in the other ten non-EU member states to which favourable treatment has been given.

In fact, the U.S. has already implemented a liberalisation of export controls on encryption products from 19 October 2000. Under the new U.S. policy announced on 17 July 2000,[76] U.S. companies can export without need of a license any encryption product to any end user in the 15 nations of the EU as well as Australia, Norway, Czech Republic, Hungary, Poland, Japan, New Zealand and Switzerland. US exports are permitted to ship their products to these nations immediately after they have submitted a commodity classification request for their product to the Department of Commerce. Exports thus no longer have to wait for a completed technical review or incur a 30-day delay to ship their encryption products to customers in these countries.

In Norway an application for a three years' general licence[77] may be made for export by a named exporter of controlled goods to countries of the European Union and to the other countries[78] that adhere to all multilateral regimes on dual-use items and technology.[79]

---

75. See Regulation 1334/2000, Article 2(b)(iii).
76. See U.S. official statement at http://crypto.radiusnet.net/archive/papers/us-crypto-up.html, last visited 31.08.2001.
77. This is not to be confused with the general licence that may be issued within the European Union in terms of Regulation 1334/2000. Norway, though a member of the European Economic Area, is not part of the European Union.
78. i.e. Australia, Canada, the Czech Republic, Hungary, Japan, New Zealand, Poland, Switzerland and the U.S.
79. This information was obtained following an informal discussion with a representative of the Norwegian Foreign Ministry, November 2000.

3.2.3.2 Controls on Imports and use

The other type of control on encryption is domestic control and may involve the requirement for encryption keys and sensitive information to be handed over to third parties (which in many cases are government agencies). Such controls are controversial and have been seen to impinge on basic rights such as the right to personal privacy, freedom of speech and the right of association, as well as raising questions about the power of governments to carry out *ad hoc* searches.[80]

Most EU Member States have no restrictions on the use or import of cryptography. Neither has Norway. Some have minor controls[81] such as ordering that encrypted data be converted into an intelligible form following a police search and seizure[82] while other countries[83] have gone a step further and require that, in such search and seizure situations, the decryption key itself should be provided.

However, in Spain, although the General Telecommunications Law of 24 April 1998 provides that all information transmitted across telecommunications networks can be encrypted, there is a provision which states that if encryption is used for confidentiality, an obligation could be imposed to notify the use of the algorithm or whatever encryption procedure is used, with an effect to control it. Some[84] have warned that this provision might lead to mandatory key escrow or key recovery.

---

80. See Kennedy, G., "Encryption Policies: Codemakers, codebreakers and rulemakers: Dilemmas in current encryption policies", [2000] *CLSR* Vol. 16 no. 4, p. 240.
81. **Austria** forbids encryption in internal company and organisation radio transmissions. Similarly, **Sweden** regulates the use of cryptography in decoding equipment for encoded transmission of radio and television programmes. In **Italy**, a law demands accessibility of encrypted records for the treasury.
82. In **Ireland**, where there are reasonable grounds to suspect that an offence has been committed under the Electronic Commerce Act 2000, the judge can issue a search warrant which authorises investigation officers to require that any encoded message be put into intelligible form. The law specifically states that it is not requiring the disclosure or enabling the security of codes, passwords, algorithms, private cryptographic keys. Similarly, in **The Netherlands** if encrypted information is found in a computer during a house search, the police can order anyone who can reasonable be supposed to know the means of encryption to decrypt the information.
83. In the **United Kingdom**, there is a power to order disclosure of encrypted data in the Regulation of Investigatory Powers Act 2000, where this is necessary *inter alia* in the interest of national security, crime prevention or detection. The person in possession of the decryption key may be required to provide the decryption key itself, but not a key that is only used s an electronic signature key.
84. See the website of Fronteras Electronicas at http://www.gilc.org/crypto/spain/gilc-crypto-spain-798.html, last visited 31.08.2001.

France has restricted the domestic use and supply of cryptography for a long time but, following a speech by Prime Minister Jospin in January 1999,[85] the controls on domestic use of cryptography were relaxed.[86]

There are no controls on imports of cryptography in the U.S. and as regards domestic use, the only restrictions at the moment are penalties for circumventing copyright-protection systems.

3.2.3.3 Further updated information

It must be emphasised that the area of encryption control and regulation is vast and constantly changing. Therefore when the time comes to integrate encryption into the MEIT tool, one should carefully check for new developments and legal requirements or controls, both at an international and on a regional and national[87] level, to the export, import and use of encryption technology. If encryption software is going to be used and/or downloaded, care should be taken by the MEIT maritime service provider ("MSP") that this does not infringe international, EU or national laws.

Information on the status of cryptographic laws may be found in a number of publications[88] and online sites such as the following:

- The Wassenaar home page at http://www.wassenaar.org contains links to national organisations dealing with encryption regulation.[89]
- The OECD's Group of Experts on Information Security and Privacy from time to time carries out inventories on the controls on cryptography technologies. These are usually available online at http://www.oecd.org/dsti/sti/it/secur/.
- The Crypto Law Survey contains a periodically updated country by country analysis of encryption controls at http://cwis.kub.nl/~frw/people/koops/lawsurvy.htm. The current version at the time of writing is Version 19 of July 2001.

---

85. See the QuickLinks website at http://www.qlinks.net/quicklinks/ql990122.htm#3503, last visited 31.08.2001.
86. For further detail, see the report on France in Bert-Jaap Koops' home page – Crypto Law Survey at http://cwis.kub.nl/~frw/people/koops/cls2.html, version 19 of July 2001, last visited 31.08.2001.
87. particularly the national law of those countries from which the Application Service Provider of the MEIT tool wants to accept registration.
88. E.g. Baker, S. A. *supra* n. 48, with updates available electronically.
89. For example, for updates on controls in Germany refer to the website of the Federal Export Office (Bundesausfuhramt (BAFA)) at the Ministry of Economics at http://www.bafa.de, last visited 31.08.2001.

- The Electronic Privacy Information Centre on Cryptography and Liberty 2000 contains an international survey of encryption policies at the following URL address http://www.epic.org/crypto/intl.
- The Global Internet Liberty Campaign contains an extensive survey at http://www.gilc.org/crypto/crypto-survey.html#country.

3.2.3.4 Considerations for the Virtual Organisation

To determine which cryptography law or laws effect, if at all, the operation of a virtual organisation such as through use of the MEIT tool, when in the future, it is being considered to include cryptography as an additional security feature of the tool, a number of questions should be asked, such as the following:

(i) It is presumed that each user would have to have some kind of enduser cryptographic product. What kind of cryptographic hardware or software products are required?

(ii) What legal restrictions are there, if at all, on the use, importation and/or export of such software or hardware products?

(iii)Is this software going to be downloaded? If so, is the act of downloading deemed to be an "export" of the software and hence restricted?[90]

One would thus have to examine:

(i) the law of the country where the user is located, to see if there are any restrictions on the domestic use and/or importation of the cryptographic software or hardware;

(ii) where such software or hardware is to be exported, the law of the country from which the software or hardware is to be exported, to see if there are any export restrictions.

Another factor to be examined is whether the private/public key generation is carried out at the central MEIT server, wherever that may be located.[91] If this is the case, a record of the keys should be kept. If so, there could be implications and constraints on the holding of such a record under data protection laws, especially if one can link a particular key with its real life owner through, for example, some cross-reference or index.

---

90. See Section 3.2.3.1.2 for the EU position on this.
91. At the moment, while the prototype is being developed by IWI, the server is located at IWI's premises in Saarbrücken. It is presumed that if the tool is further developed, at a later stage after the end of the MARVIN project, into a commercial tool, the location will be that chosen by the Maritime Service Provider, whoever that person may be.

3.2.3.5 Key Management

A potential service offeror (e.g. ship repair yard, classification society, salvage company) or user (shipowner or ship manager) of the MEIT system will first have to register with the system[92] and provide certain information (which could also include confidential information) on their areas of operation, fields of expertise, etc. Information that will help to identify the "real-world" identity of such applicant should also be requested. It is advised that,[93] once the applicant's identity is confirmed as explained in Section 3.2.4.1 below, an account (and a user name) are generated for that user. The user could be requested and allowed to select a password for his use, with an obligation that such password should be kept secret.

Correct management of keys is an essential aspect of any cryptographic system. As Brazell explains,[94] apart from the initial function of generating keys, there must also be means for:

(i) establishing or verifying the real world identity of the keyholder;

(ii) enabling distribution by publication or secure exchange (depending on whether public or private key encryption is being utilised) of keys to those who need and are entitled to have them;

(iii) revocation of keys whose security is suspected to have been compromised by any means, and of letting those who need to know with certainty of the revocation;

(iv) the multitude of keys any one user will need must also be safely stored and indexed for use as required.

3.2.4 Digital Signatures and Certification

3.2.4.1 Authentication

Thus, the "real world" identity of the applicant should be verified. Verification can be carried out either:

i. off-line, i.e. a trusted person such as a notary or a public official attests to the identity of the applicant;

ii. electronically through, for example, a digital signature which is certified by a certification authority. In fact, this is sometimes also referred to as

92. See *supra* n.41, at Section 2.1.
93. especially in the commercial version of the MEIT system.
94. Brazell, L., *supra* n. 45, p. 19.

the "electronic notarisation" of a document. This assumes, however, the following:

i. that the MEIT will allow the digital signature of an application;

ii. that the applicant has the technology which enables him/her to produce a digital signature;

iii. that the applicant has access to the services of a certification authority.

Other constraints to electronic certification could be legal constraints in the form of domestic regulation and controls of certification authorities and of the extent to which a digital signature which has been certified by a foreign certification authority would be legally recognised and valid. One would have to see, for example, what would be the status of a digitally signed document, i.e. whether it would be considered to be a "writing" and "signed". Below is some information on the situation in the EU.

3.2.4.2 The EU Electronic Signatures Directive

The need for ensuring legal recognition, in particular across borders, of electronic signatures and of certification services has been addressed by the EU in its Electronic Signatures Directive.[95] This Directive recognises the legal validity of electronic signatures and tries to establish a legal framework for the operation of Certification Service Providers.

According to the Directive, Member States are to ensure that advanced electronic signatures which are based on a qualified certificate and which are created by a secure-signature-creation device,[96] (a) satisfy the legal requirements of a signature in relation to data in electronic form in the same manner as a handwritten signature satisfies those requirements in relation to paper-based data, and (b) are admissible as evidence in legal proceedings. It also provides that an electronic signature should not be denied legal effectiveness or admissibility solely on the ground that it is in electronic form, or not based upon a qualified certificate, or not based upon a qualified certificate issued by an accredited certification-service-provider, or not created by a secure signature-creation device.[97]

---

95. Directive 1999/93/EC of the European Parliament and of the Council of 13 December 1999 on a Community framework for electronic signatures (the "Electronic Signatures Directive"), O.J. L 13, 19.01.2000, p. 12, available at http://europa.eu.int/eur-lex/en/lif/dat/2000/en_300L0031.html, last visited 31.08.2001.
96. It is expected that hardware will also be required to generate a qualified electronic signature.
97. See Article 5, Electronic Signatures Directive, *supra* n. 95.

The deadline for Member States to comply with the Directive was before 19 July 2001,[98] and in fact, a number of EU and EEA Member States are introducing legislation to implement this Directive[99] or to bring their current laws in line with this Directive where there were legal provisions on this matter.[100]

The Directive provides that Member States may not restrict the provision of certification services originating in another Member State in the fields covered by this Directive. As regards qualified certificates issued in a country outside the EU, these should be recognised as legally equivalent to certificates issued within the Community where:

(a) the Certification Service Provider fulfils the requirements of the Directive and has been accredited under a voluntary accreditation scheme established in a Member State, or

(b) a Certification Service Provider established within the Community which fulfils the requirements laid down in the Directive guarantees the certificate, or

(c) the certificate or the Certification Service Provider is recognised under a bilateral or multilateral agreement between the Community and third countries or international organisations.[101]

The field of digital signature regulation, like that of encryption, is also vast and in constant change. Information on the status of cryptographic laws may also be found in a number of online sites such as the OECD's site at http://www.oecd.org/dsti/sti/it/secur/ and the site of the Digital Signature Law Survey at http://www..kub.nl/simone/ds-lawsu.htm.

98. Article 13, Electronic Signatures Directive, *supra* n. 95.
99. For example, the Norwegian Act on Electronic Signatures entered into force on 1st July 2001, see Lov om elektronisk signatur 15. Juni 2001 nr. 81.
100. A number of proposed amendments to the German Digital Signature law were approved by the Federal Cabinet in Germany on August 16, 2000, the main purpose of which is to implement the EU Electronic Signatures Directive. For a translation of this draft law, see the translation by Christopher Kuner, online at: http://www.kuner.com, last visited 31.08.2001.
101. See Article 7, Electronic Signatures Directive, *supra* n. 95.

4. THE USERS AND THE MEIT: THE MEIT USER AGREEMENT

4.1 Introduction

Various references[102] have already been made to the need of having certain provisions in an on-line MEIT User Agreement, the terms and conditions of which every user of the MEIT, be it a service offeror (e.g. shipyard, salvage company, classification society, etc.) or the client/customer of the service offeror (i.e. the shipowner or ship manager) should agree to upon registering in the system.[103]

Such an agreement is important since it would regulate the relationship between the users of the MEIT and the person maintaining the MEIT system (the maritime service provider). Such an on-line contract would contain certain terms and conditions which one usually finds in agreements with an international character (since it is hoped that the parties thereto will be from various countries, both from within and outside the EU), such as:

- intellectual property clause: The user should respect the intellectual property rights in the MEIT, in any other software provided to the user (e.g. interfaces), and in the website maintained by the MEIT application service provider.
- choice of law clause: Should there be an express choice of law? Which is the law in terms of which the agreement is to be construed and interpreted?
- choice of forum clause: What is the benefit of having such a clause? Which country's court should have jurisdiction to hear disputes arising from use of the system?
- limitation of liability clause: To what extent should and could liability for defects/errors of the MEIT be limited?

The novelty and also the difficulty that arises in this context is that since it is envisaged that the MEIT will be accessible and available for the "on-line public at large" (i.e. to anyone who has an Internet connection), then unless certain fundamental principles have been agreed to beforehand by the potential users of the tool through some kind of general form agreement such as the

---

102. See in particular Section 2.3.
103. In this way, someone who is not willing to adhere to the level of security of, and terms and conditions of use of, the MEIT, would be kept out of the system rather than accepted as a user with the risk that the level of security and reliability of the MEIT could be jeopardised.

MEIT User Agreement, if a dispute arises from the use of the tool, a vast number of different legal systems could vie with each other as to the definition of the relationship that the users of the system have with the system and with each other.[104]

A number of draft clauses for such a MEIT User Agreement are proposed in Appendix 4. These (or most of these) draft clauses could be put together, refined and tailored further according to how the final commercial MEIT system has been developed, and then used as the MEIT User Agreement. However, it is should be cautioned that the proposed draft clauses cannot be taken to be the final word on how the MEIT User Agreement would or should look. This is due to a number of factors, the principal of which being that the main task of the MARVIN project is to develop a *prototype* software[105] and not a finished product which has been developed, tested and ready for commercial use. The clauses proposed in Appendix 4 should therefore be taken as illustrative clauses that could be adapted for use in a situation similar to that explained in this study.

It is being assumed that the intellectual property developed in the MARVIN project will be transferred[106] to a maritime service provider – hereinafter referred to as an MSP – that will be selected by the MARVIN partners. The main tasks of the MSP would be (i) to see to the development of the MEIT prototype into a commercial tool and, once this has been achieved, (ii) to operate and maintain the MEIT as its service provider.

To be attractive to an MSP, a commercial version of the MEIT system should be capable of generating income for the MSP. This could be done in a number of different ways, such as the following:

(i) there could be a commission earned on the gross value of the transactions made via the MEIT system (e.g. where a shipowner has contracted a shipyard, the fee could be a commission of, say, 1 per cent of the total contract fees);

(ii) there could be a periodical (e.g. annual) subscription fee for all users of the MEIT, operative from registration with the system;

(iii) a combination or variation of (i) and (ii) abovementioned.

---

104. Moreover, in the maritime field, in particular with regards to the first scenario – that of emergency repair - being examined in this project, casualties can happen anywhere, both in territorial waters and also on the high seas.
105. Moreover, this prototype software is currently still under development.
106. The manner and terms of such transfer (e.g. whether this should be against a fee and how much) have also not yet been determined.

At the time of writing it is difficult to propose a clear payment/charges/commission clause(s) in Appendix 4. Therefore, only a simple draft of a commission clause is proposed in draft Clause 19. Once a business plan has been drawn up, it should not be too difficult to draft such a clause(s).

Moreover, since, of course, an MSP has not as yet been identified or selected, it is difficult at this stage to specify and choose the governing law and jurisdiction of this Agreement. Nevertheless, the issues of choice of law and jurisdiction are discussed below in Section 4.5 where it will be recommended that there should be an express choice of law and jurisdiction clause, and Section 4.5.4 proposes a factor that could be used as a basis to choose the governing law and forum. The format for a choice of law and jurisdiction clause are proposed in Clause 18 (with a blank space for insertion of the country whose law and jurisdiction have been chosen).

The proposed draft clauses are therefore not to be taken as the final word on what the MEIT User Agreement should look like, nor are they to be taken as legal advice. They are put forward to give a feeling of what such an agreement could look like, and are not final. These draft clauses should be examined and developed further in the light of the chosen law, the business and exploitation plans (once these have been finalised), and all other factors that may arise by the time the MEIT prototype has been developed into a commercial tool.

4.2 Web contracting

4.2.1 Internet contracting

In recent years, a new kind of contract has gained widespread use in the acquisition of off-the-shelf software: the shrink-wrap contract. Such software products, encased in shrink-wrapped transparent plastic, usually contain a standard pre-printed software licence contract on the outside of the box (or on a card inside the box). By performing a certain act (e.g. opening the shrink-wrap or loading/installing the software on his/her computer system), the user is deemed to have accepted the conditions of the pre-printed licence terms.

On the Internet, a new kind of shrink-wrap licence is becoming common: the "click-wrap" contract. In fact, on the Internet standard term contracts[107] are likely to be even more frequent than in other contexts. A click-wrap con-

107. These are also referred to in jurisprudence as contracts of adhesion.

tract is displayed on the computer screen and asks the user to "Click here if you agree to be bound by the terms and conditions of the agreement." By clicking their mouse on the small box marked "I Agree", users are deemed to have agreed to the terms and are allowed to proceed.

Naturally, the question that arises is whether such click-wrap contracts are validly entered into and enforceable. The legal validity of click-wraps and shrink-wraps, as Burnstein explains,[108] has long been uncertain but recently courts have begun to take a favourable approach, suggesting that click-wrap choice of law clauses will be honoured. The United States Court of Appeals for the Seventh Circuit in 1996 upheld the use of a click-wrap licence in ProCD Inc. v. Zeidenberg,[109] and a Scottish court upheld a shrink-wrap contract in Beta Computers v. Adobe Systems. The implication of these cases for Internet contracts is that, if users can be bound by a click-wrap agreement, then Web sites and retailers can better control where they must face litigation and whose law applies to such suits.

One should here mention that the Electronic Commerce Directive[110] calls upon EU member states "to ensure that their legal system allows contracts to be concluded by electronic means." More importantly, this means that EU Member States have to "in particular ensure that the legal requirements applicable to the contractual process neither create obstacles for the use of electronic contracts nor result in such contracts being deprived of legal effectiveness and validity on account of their having been made by electronic means".[111] Thus, it is to be expected that, at least within the 15 EU Member States, electronic contracts will not run the risk of being deemed invalid or without legal effect simply because they have been made by electronic means. This Directive, in force since 17 July 2000, should be implemented by member states before 17 January 2002.

---

108. See Burnstein, M., "A Global Network in a Compartmentalised Legal Environment", in *Internet: Which Court Decides? Which Law Applies? Quel tribunal décide? Quel droit s'applique?*, Boele-Woelki & Kessedjian eds., 1998, Kluwer Law International , para 2.2.3.
109. 86 F.3d 1447 (7th Cir. 1996).
110. Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market, O.J. L 178, 17.7.2000, hereinafter referred to as the "Electronic Commerce Directive", available at http://europa.eu.int/eur-lex/en/lif/dat/2000/en_300L0031.html, last visited 15.08.2001.
111. Article 9(1), Electronic Commerce Directive, *supra* n. 110.

The following actions[112] will increase the probability that a contract is deemed to be enforceable and it is recommended that the MEIT system should implement such actions:

(i) implement software to try to prevent a user from registering until all registration information has been provided by the user;

(ii) require the user to go through the contract term screens before he/she may proceed with registration on the system;

(iii) provide the user with the option to leave the contract screen sequence at any point;

(iv) require the user to indicate consent to the contract terms in an affirmative, unambiguous way which demonstrates that he/she agrees to the displayed terms. For example, after showing the contract term screens, direct the user that to indicate contract acceptance, he/she must click in a designated box with the words "I accept" written thereon, or by typing a character string like "I _____, hereby accept the contract terms of MEIT." (The blank line is for the user to fill in his/her full name.)

(v) maintain a well organised record of user acceptance of agreement terms by keeping a log of the sequence of contract screens shown to each applicant together with the user's acceptance response.

The MEIT User Agreement being proposed is a type of web contract which all persons registering for the first time with the MEIT should accept to become a party to. The way a web contract such as the MEIT User Agreement would work is as follows: Before registering with the MEIT, the user would be guided to a screen where the MEIT User Agreement appears. The user is then made to scroll through all the terms and provisions of this Agreement and then given an option either to agree or not to agree to its terms and conditions. A contract is deemed to be concluded when the customer affirmatively accepts the terms of the contract. Such affirmative action could take the form of the user clicking on the "I agree" button on the screen after having read the terms and conditions of the agreement.

What should definitely be avoided is to have a separate web page with so-called general term and conditions of the contract, which a potential user of the MEIT is at liberty to view or not view before clicking on the "I agree" button. This would raise difficulties as to whether such a user was actually aware

112. See Greguras, F. M., Golobic, T. A., Mesa, R. A. and Duncan, R., *Electronic Commerce: On-line Contract Issues* at http://www.batnet.com/oikoumenc/ec_contracts.html, last visited 31.08.2001.

of all these terms and conditions before sending his/her acceptance, and whether such terms, especially the more onerous ones, are applicable to such user. This matter has already been discussed in legal literature dealing with standard term contracts and reference is here made thereto.[113] Therefore, to recapitulate, it is essential that a potential user has good opportunity to see and read all the contractual terms by scrolling down the screen before he/she agrees to such terms.

Of course, the user should also be asked to input details – perhaps through a pop-up screen with blank fields for input by the user - to identify him/her such as name, address, telephone, fax, e-mail, details of contact person, etc. (Clause 4 in the sample clauses in Appendix 4 deals with registration obligations and Clause 5 deals with the allocation of a user name by the MSP and the selection of a password by the user.)

4.2.2 Information to be provided by the maritime service provider

If the MEIT maritime service provider is established inside the European Union – as is at the moment envisaged - it should comply with the provisions of the Electronic Commerce Directive[114] since it would appear to fall within the ambit of the Directive. The Directive applies to the provision of information society services which include services giving rise to on-line contracting, and include services consisting of the transmission of information via a communication network, the provision of access to a communication network or the hosting of information provided by a recipient of the service (Recital 18).

This Directive requires a service provider such as the MSP to render easily, directly and permanently accessible to the recipients of the service and competent authorities at least the information laid down in Article 5 thereof, which includes the following:

(a) the name of the service provider;

(b) the geographic address at which the service provider is established;

(c) the details of the service provider, including his electronic mail address, which allow him to be contacted rapidly and communicated with in a direct and effective manner;

113. See, for example, Beale, H.G. (ed.), *Chitty on Contracts*, Vol. 1 General Principles, 28th ed., Sweet & Maxwell, London, 1999, para. 12-008-12-018.

114. See *supra* n. 110.

(d) where the service provider is registered in a trade or similar public register, the trade register in which the service provider is entered and his registration number, or equivalent means of identification in that register;

(e) where the service provider undertakes an activity that is subject to VAT, the identification number;

(f) where information society services refer to prices, these are to be indicated clearly and unambiguously and, in particular, must indicate whether they are inclusive of tax and delivery costs.

Such information should be clearly and permanently displayed on the web site of the MEIT MSP.

In addition, commercial communication[115] which is part of, or constitutes an information society service, should comply with the conditions of Article 6 of the Electronic Commerce Directive. For the services envisaged to be provided by the MEIT, the following conditions are perhaps mostly relevant:

(a) the commercial communication shall be clearly identifiable as such;

(b) the natural or legal person on whose behalf the commercial communication is made shall be clearly identifiable;

(c) promotional offers are to be clearly identifiable as such.

The proposed draft Clause 7(4) in Appendix 4 is meant to reflect the above.

The MEIT MSP should also bear in mind that unsolicited commercial communication by electronic mail, where permitted in an EU Member State, should be identifiable clearly and unambiguously as such as soon as it is received by the recipient.[116]

---

115. The term "commercial communication" is defined in Article 2(f) of the Electronic Commerce Directive as "any form of communication designed to promote, directly or indirectly, the goods, services or image of a company, organisation or person pursing a commercial, industrial or craft activity or exercising a regulated profession. The following do not in themselves constitute commercial communications:
-information allowing direct access to the activity of the company, organisation or person, in particular a domain name or an electronic-mail address,
-communications relating to the goods, services or image of the company, organisation or person compiled in an independent manner, particularly when this is without financial consideration."

116. See Article 7(1) of the Electronic Commerce Directive and Article 7(2) which also mentions the obligation of service providers to regularly consult and respect opt-out registers in which natural persons not wishing to receive such commercial communications can register themselves.

The Electronic Commerce Directive also lays down, in Articles 10(1)(2)[117] and 11[118], other information that should be provided and formalities that should be followed prior to any order being placed by the recipient of the service. The Directive, however, allows parties who are not consumers to agree otherwise.

Since, according to the Electronic Commerce Directive, "contract terms and general conditions provided to the recipient must be made available in a way that allows him to store and reproduce them",[119] it should be technically possible for the MEIT User to be able to store and reproduce the Agreement.

4.3 Evidentiary issues

Although, as we have seen above in Section 4.2, within the territories of the European Union, it is to be expected that electronic contracts will not be

117. Article 10(1)(2) provides that:
"(1) In addition to other information requirements established by Community law, Member States shall ensure, except when otherwise agreed by parties who are not consumers, that at least the following information is given by the service provider clearly, comprehensibly and unambiguously and prior to the order being placed by the recipient of the service:
(a)the different technical steps to follow to conclude the contract;
(b)whether or not the concluded contract will be filed by the service provider and whether it will be accessible;
(c)the technical means for identifying and correcting input errors prior to the placing of the order;
(d)the languages offered for the conclusion of the contract.
(2)Member States shall ensure that, except when otherwise agreed by parties who are not consumers, the service provider indicates any relevant codes of conduct to which he subscribes and information on how those codes can be consulted electronically."

118. Article 11 provides that:
(1)Member States shall ensure, except when otherwise agreed by parties who are not consumers, that in cases where the recipient of the service places his order through technological means, the following principles apply:
- the service provider has to acknowledge the receipt of the recipient's order without undue delay and by electronic means,
- the order and the acknowledgement of receipt are deemed to be received when the parties to whom they are addressed are able to access them.
(2)Member States shall ensure that, except when otherwise agreed by parties who are not consumers, the service provider makes available to the recipient of the service appropriate, effective and accessible technical means allowing him to identify and correct input errors, prior to the placing of the order.
(3)Paragraph 1, first indent, and paragraph 2 shall not apply to contracts concluded exclusively by exchange of electronic mail or by equivalent individual communications."

119. Article 10(3).

deprived of legal effect and validity simply on account of their having been made by electronic means, the situation may not be so clear as regards other jurisdictions. It is therefore being recommended that a clause be inserted in the MEIT User Agreement whereby the users agree to the legal validity and effect and evidentiary value of electronic contracts. The suggested clause in Appendix 4 on validity of electronic contracts – Clause 10(1) - is loosely based on Article 3.1 of the European Model Electronic Data Interchange (EDI) Agreement,[120] whereas Clause 11 on equivalence of data messages to writing or paper documents is based on Clause 17(1) of the UNCITRAL Model Law on Electronic Commerce of 1996.[121] Clause 10(1) provides:

> *"You agree to be legally bound by the terms of this Agreement and expressly waive any rights to contest the validity this Agreement or of any other contract effected through this Service with any other User of this System on the sole ground that it was effected electronically."*

Clause 11 provides:

> *"Where any action is required by any Users of the System to be carried out in writing or by using a paper document, either between the Users and the System or between the Users themselves, such requirement is met if the action is carried out by using one or more Data Messages."*

The difficulty that could arise with a clause such as clause 10(1) is that it could be considered to be a stipulation for the benefit of a third party (insofar as the MEIT User Agreement is a contract between the MEIT MSP and each individual user), and a number of legal systems do not always enforce such stipulations. What could be done to perhaps obviate this problem is to bind each user to include a clause, in its separate electronic agreements with other users of the MEIT, that upholds the legal validity of electronic contracts and recognises the equivalence of data messages on lines similar to Clauses 10(1). Such would be a provision like draft Clause 10(2), viz.:

> *"(2) You undertake and bind yourself to include a clause in any and all electronic agreements that you may enter into with any other User or Users of this System whereby you expressly waive any right to contest the validity of such electronic agreement on the sole ground that it was effected electronically."*

---

120. 94/820/EC: Commission Recommendation of 19 October 1994 relating to the legal aspects of electronic data interchange (Text with EEA relevance), O.J. L 338 , 28/12/1994. pp. 0098 – 0117.
121. See *supra* n. 38.

These aforementioned two draft clauses are reminiscent of typical or traditional EDI-related issues. In fact, other EDI-related issues should be included in such agreement (or in a Technical Annex to the MEIT Agreement) such as the keeping of a log and the storage of electronic messages, and specifications of what types of digital signatures are deemed to be secure electronic signatures according to the Agreement (of course, once digital signature technology has been incorporated as an additional security feature of the MEIT).

4.4 Security and confidentiality

The need to ensure security of the MEIT system and confidentiality of the data transmitted via the MEIT has already been examined in Chapter 3. Draft clause 5 in Appendix 4 deals with the generation of a user name by the MSP which will be communicated to the MEIT user once the real world identity of the proposed user has been confirmed (see Sections 3.2.3.5 and 3.2.4.1 above), and the selection of a password by the user.

4.5 Choice of law and Choice of forum

One of the revolutionary features of Internet communication is that distance has become irrelevant. A message from a user in Hamburg to a server in Saarbrücken is no different to a message from a user in Lisbon to the same server. Once a user has access to the Internet, it is irrelevant where that user is located. The novelty of the Internet is that it ignores traditional geographical boundaries. "Place" has little meaning in the networked world.[122]

Traditional private international law has looked to geography when selecting the applicable law and determining jurisdiction. Article 4(1) of the 1980 Rome Convention[123] and Article 3 of the 1955 Hague Convention[124] and Article 5(3) of the 1868 Brussels Convention[125] ask questions such as: "Where is the habitual residence of the party who is to effect the performance of the contract? Where has the order been received? Where has the harmful event

122. For an excellent discussion of the new challenges posed to traditional private international law principles such as choice of law, see Burnstein, M., *supra* n. 108.
123. EC Convention on the Law Applicable to Contractual Obligations (Rome 1980) - the "1980 Rome Convention", O.J. C 027, 26/01/1998, pp. 0034 – 0046, also available at http://www.jus.uio.no/lm/ec.applicable.law.contracts.1980/doc.html, last visited 31.08.2001.
124. Convention on the Law Applicable to International Sale of Goods, The Hague, 1955 - the "1955 Hague Convention", available at http://www.ulcc.ca/en/us/?sec=1&sub=1l&print=1#2, last visited 31.08.2001.

occurred?" However, on the Internet, "place" matters less and less and it is often difficult, in the absence of an express choice of law by the parties, to determine which is the applicable law to govern a particular contractual relationship. For example, does the mere accessibility of digital matter available on the MEIT web browser by the users of the MEIT subject such users to the laws and sanctions of the country where the communication originates, where it traverses, where it terminates, or all three?

4.5.1 Where there is no express choice of law

The question arises whether there is need for an express choice of law in the MEIT User Agreement. Perhaps one way to try and answer this question is to examine what is the position where there is no express choice of law by the parties to the contract, i.e. what happens where the parties have not expressly chosen the law in terms of which the contract should be construed and interpreted.

According to Article 4(1) of the 1980 Rome Convention, if the parties to a contract have not agreed to apply a particular law to govern that contract, the contract is deemed to be governed by the law of the country with which it is most closely connected. This is presumed to be the place of business or the habitual residence of the party who is to effect the characteristic performance (Article 4(2)). In questions of carriage of goods (carriage under bills of lading or single voyage charterparties), this presumption does not apply and is replaced by the law of the place where the carrier has his principal place of business, if it is also the place of loading or discharge or the place where the shipper has his principal place of business (Article 4(4)).[126] This presumption is rebuttable (Article 4(5)).

What about questions arising between MEIT users who are offering services and the shipowner/ship manager? The court would have to look for "connecting factors" to determine which is the law which is to govern that particular contract. In a maritime scenario there may be a variety of such factors, viz.:

---

125. EC Convention on Jurisdiction and the Enforcement of Judgments in Civil and Commercial Matters, Brussels 1968 (Full Faith and Credit Convention) - the "1968 Brussels Convention", O.J. L 299, 31/12/1972, pp. 0032 – 0042, also available at http://europa.eu.int/eur-lex/en/lif/dat/1968/en_468A0927_01.html, last visited 31.08.2001.
126. Tetley, W., *International Conflict of Laws: Common, Civil and Maritime*, 1994, Blais, p. 233.

(i) the law of the flag of the vessel: Is this to be interpreted to be the law of the ship's registry and if so, what happens when there are double registries or double flagging? In a federal state, which is the law that applies?

(ii) the law of the place of business of the shipowner.

Germany, Greece, The Netherlands and Portugal are signatories of the 1980 Rome Convention but Norway is not a party to this Convention.[127] In Norway, contracts are governed by the law chosen by the parties or, failing agreement, by criteria depending on the nature of the contract. The Convention's principle of "the most significant relationship" has been established in an early Norwegian Supreme Court decision, Irma-Mignon.[128]

In the case of an international sale of goods contract then according to the 1955 Hague Convention, in default of an express choice of law by the parties, the sale is deemed to be governed by the domestic law of the country in which the vendor has his habitual residence at the time when he receives the order (Article 3(1)). However, if the order has been received in the country where the purchaser has his habitual residence, the contract shall be governed by that law.

Thus, where there is no express choice of law, it could be a complex matter for the court seized of a matter to determine which is the applicable law to govern the agreement between the parties.

4.5.2 Express choice of law and choice of forum

Writers on Internet law believe that the most effective way to resolve Internet private international law problems is to use choice of law and choice of jurisdiction clauses in contracts among users and Internet service providers as a means of agreeing to a common choice of law, rather than leaving it to the uncertainties of geographically-oriented choice of law regimes.[129] As Kronke observes, free choice of governing law, the basic principle of the 1980 Rome Convention, is the easiest and most efficient way to solve the problems facing us.[130]

A standard choice of law clause would read something like the following: "This agreement shall be governed by and construed in accordance with the

127. These are the five countries where the MARVIN project partners are established.
128. Rt. 1923 II, p. 58, quoted by Tetley, W. *ibid*.
129. See Burnstein, M., *supra* n. 108, para. 2.2.1
130. See Kronke, H. "Applicable Law in Torts and Contracts in Cyberspace", *Internet: Which Court Decides? Which Law Applies? Quel tribunal décide? Quel droit s'applique?*, Boele-Woelki & Kessedjian eds., 1998, Kluwer Law International, para 3.3.1 (a).

laws of X [usually the place of business of the service or content provider]". As observed by Burnstein[131],

> *"forum and law selection clauses in online service contracts can bring order and stability to choice of law for Internet disputes by substituting an agreed-upon law for the uncertain and patchwork regime likely to result if courts are left to guess at what law should apply."*

Choice of law clauses have become widely-accepted. Article 3(1) of the 1980 Rome Convention allows the parties to choose any law irrespective of whether it has any connection with the contract or the parties - of course, provided that the choice is expressed or can be demonstrated with reasonable certainty by the terms of the contract. Article 2 of the 1955 Hague Convention also provides, with regards to international sale of goods, that where the parties have expressly or unambiguously chosen the law to govern that contract, the sale will be governed by that law.

Similarly, with regards to choice of forum clauses, which are also widely used in contracts, the 1968 Brussels Convention[132] provides that if the parties have agreed that a court or the courts of a contracting state are to have jurisdiction to settle any disputes which have arisen or which may arise in connection with a particular legal relationship, that court or those courts shall have exclusive jurisdiction, provided this agreement of the parties is either in writing or evidenced in writing or, in international trade or commerce, in a form which accords with practice in that trade or commerce of which the parties are or ought to have been aware (Article 17).

In an online environment, the question that immediately arises is whether a jurisdiction clause in an electronic contract such as the MEIT User Agreement can be deemed to fall within Article 17 of the Brussels Convention. Is it a "writing or evidenced in writing"? The difficulty arises because the Brussels Convention should be interpreted restrictively and because it was obviously not written with the online environment in mind in 1968! It is submitted that a court would deem such an electronic clause to be in writing or evidenced in writing if the Agreement in which it is contained has been filed, is durable and

131. Burnstein, M., *supra* n. 108, para. 2.2.1.

132. All the EU Member States have signed the Brussels Convention. Although Norway is not a signatory, it is a member of the 1988 Lugano Convention on Jurisdiction and the Enforcement of judgments in Civil and Commercial Matters, which is open for signature also to non-EU Member States and is a parallel and identical convention to the Brussels Convention. The Lugano Convention is available in O.J. No. L 319 , 25/11/1988, pp. 0009 – 0033, and also at http://europa.eu.int/eur-lex/en/lif/dat/1988/en_488A0592.html, last visited 31.08.2001.

is accessible to both parties and hence could be produced in evidence. The Electronic Commerce Directive also obliges EU Member States to ensure that contracts can be concluded by electronic means and are not to be deprived of legal effectiveness or validity just because they were made by electronic means.[133] However, this difficulty has been superceded by the recent Council Regulation (EC) No 44/2001 of 22 December 2000 on jurisdiction and the recognition and enforcement of judgments in civil and commercial matters,[134] Article 23(2) of which provides:

> *"Any communication by electronic means which provides a durable record of the agreement shall be equivalent to 'writing'".*

As was mentioned in Section 4.2 above, in the last decade a new kind of contract – the "click-wrap" contract has become increasingly popular as a web contract, with the courts becoming increasingly willing to uphold such contracts.

4.5.3 The EU Directive on Distance Contracts

At this outset one should briefly examine whether the EU Directive on Distance Contracts[135] is applicable to the particular MEIT virtual enterprise scenario, specifically to the agreement between the service offeror (i.e. a shipyard and/or classification society and/or tug company) or the service user (shipowner or ship manager) and the MEIT MSP.

Article 12 of the EU Directive provides that consumers may not either waive the rights granted them under this Directive either explicitly or implicitly by agreeing to apply a law which lacks the consumer protections under the Directive.[136]

A "consumer" is defined as a "natural person"[137] in Article 2(2) of the Directive. It would therefore seem that this Directive is not applicable to the

---

133. Article 9, Electronic Commerce Directive.
134. O.J. L 012, 16/01/2001, pp. 0001 – 0023. This Regulation enters into effect on 1 March 2002.
135. Directive 97/7/EC of the European Parliament and of the Council of 20 May 1997 on the protection of consumers in respect of distance contracts, O.J. L 144, 04/06/1997, pp. 0019 - 0027.
136. Article 12 of the Directive provides that:
"1. The consumer may not waive the rights conferred on him by the transposition of this Directive into national law.
2. Member States shall take the measures needed to ensure that the consumer does not lose the protection granted by this Directive by virtue of the choice of the law of a non-member country as the law applicable to the contract if the latter has close connection with the territory of one or more Member States."

abovementioned situation since neither the shipowner nor the service offeror – the users of the MEIT - are consumers in this sense, and thus such agreements fall outside the scope of this Directive. The MEIT is targeted for use by the maritime industry,[138] and the users entering into the MEIT User Agreement with the MSP will be doing so in their line of trade, busines or profession. However, if a private yacht owner were allowed to register on the MEIT system, the EU Directive would probably apply since such a person falls within the definition of a "consumer" in the Directive. If the tool is not meant for use by private individuals, then such private individuals should not be accepted as users by the system. This is another function which could be performed during the verification of the identity of a person who applies to use the MEIT.

4.5.4 Which is the applicable law?

For the reasons explained above, it is therefore submitted that there should be an express choice of law in the MEIT User Agreement. As to the question of which law should be chosen, a practical and appropriate choice is the law of the place where the marine service provider is established,[139] since this is a common denominator for operations made through the integration tool whereas other options such as the law of the user's habitual residence or domicile will obviously vary from user to user. Another practical alternative (for both choice of law and jurisdiction) would be to choose one of the laws and forums already commonly used in maritime trade, e.g. London, as such a legal system would already be very familiar to the users of the tool.

4.6 Liability issues

Another issue that arises and becomes relevant once a commercial version of the MEIT has been developed and the system is available for commercial use,

137. A consumer is defined as "any natural person who, in contracts covered by this Directive, is acting for purposes which are outside his trade, business or profession".
138. See Chapter 2 of the MARVIN Project Programme, Part 2: Description of the RTD Project.
139. Establishment is a commonly used basis for founding jurisdiction in a number of legal instruments – see, for example, the Data Protection Directive (Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and the free movement of such data, O.J. L 281 p.31, 23/11/1995), the Televisions Directive (Directive 97/36/EC of the European Parliament and of the Council of 30 June 1997 amending Council Directive 89/552/EEC on the coordination of certain provisions laid down by law, regulation or administrative action in Member States concerning the pursuit of television broadcasting activities, O.J. L 202 p. 60, 30/07/1997), the Brussels and the Lugano Conventions.

is what happens if the MEIT system malfunctions. Who would be liable: the programmer who programmed the system, the domain experts who provided the intelligence for the knowledge base of the system, the MSP, the MEIT users? To what extent would such person be liable?

According to the technical specification of the MEIT software, every agent in the MEIT operates as an expert system:

> *"Since different classes of actors exist in the focus of the MARVIN project, every agent representing a special actor of the scenario has its own knowledge base. That means every agent operates as an expert system with the goal to satisfy the needs of the enterprise it represents and the customer (ship crew and shipowner) respectively. … Different knowledge bases have to be created for classes of actors using the MEIT consequently."*[140]

To try and establish if there is liability, one would first have to examine the nature of the defect or malfunction that occurred. The following are some examples. Assuming that the partner search is automated in the commercial version of the MEIT, did the MEIT give an unfair or incorrect shortlisting of potential partner firms? Was this due to a defect in programming (by the system programmer) or because of a mistake by the domain expert who provided the knowledge for the integration tool? Was it due to erroneous or intentionally incorrect input of data by another user of the MEIT?

Before examining these issues in further detail, there is a short discussion of exclusion clauses and limitation of liability clauses.

4.6.1 The validity of exclusion and limitation of liability clauses

Two mechanisms commonly used in agreements are exclusion clauses and limitation of liability clauses. Exclusion clauses are not always given effect. In fact, national legal systems have developed specific controls over such clauses, even before the advent of specific legislation thereon, often applying rules relating to the reality of quality of consent given by the other party against whom such exclusion clause is being claimed.

For example, liability for intentional non-performance and gross negligence cannot be excluded or limited in Germany (BGB[141]§272(2)) but such clauses are valid as regards the acts of persons to whom the obligor has entrusted performance, and for whose acts he is responsible - BGB§278. A rule similar to the German BGB §276(2) is found in the Greek Civil Code Article

140. See Angeli, R., Odendahl, C., Kraus, S., *op. cit. supra* n. 5, at Section 2.2.1.
141. The BGB is an abbreviation of Bürgerliches Gesetzbuch – the German Civil Code.

332. Greek law permits exclusion clauses covering persons entrusted with performance, as does BGB §278.

In Portugal, according to the prevailing opinion, only vicarious liability may be excluded - Civil Code Articles 809 and 800 - while clauses limiting liability are valid except for intentional or grossly negligent non-performance. Under the Law of 25 October 1985 general conditions of contract exempting the defaulting party from liability for intentional and grossly negligent non-performance are invalid.[142]

4.6.2 Liability of the MEIT MSP

The practice of relying on limitation and exclusion of liability clauses is widely recognised by national laws and used in business practice.[143] It could happen that the integration tool malfunctions because of a bug or defect that produces erroneous results. To what extent would or should the MSP be liable for such defects? It is an incontrovertible fact that no software is error free and thus some limitation of liability should be acceptable and, indeed, is common in the information technology industry.

Damage could also occur where, because of some incorrect data which had been provided by a user (whether provided intentionally or otherwise), an unfair result or recommendation was arrived at by the integration tool. For example, if the partner search process is automated in the MEIT, it could happen that one user provides some incorrect data and he is given a higher ranking

---

142. Lando, O. & Beale, H., *The Principles of European Contract Law*, 1995, Martinus Nijhoff Publishers, p. 150.

143. For example, Article 8.109 of the Principles of European Contract Law 1998 provides that:
"Clause Limiting or Excluding Remedies
Remedies for non-performance may be excluded or restricted unless it would be contrary to good faith and fair dealing to invoke the exclusion or restriction."
Article 7.1.6 of the UNIDROIT Principles of International Commercial Contracts 1994 provides that:
"Exemption Clauses
A clause which limits or excludes one party's liability for non-performance or which permits one party to tender performance substantially different from what the other party reasonably expected may not be invoked if it would be grossly unfair to do so, having regard to the purpose of the contract."
A copy of the Principles of European Contract Law, drawn up by the Commission on European Contract Law under the chairmanship of Prof. Ole Lando, may be viewed at the following web address: http://www.jus.uio.no/lm/eu.contract.principles.1998/doc.html, last visited 31.08.2001. A copy of the UNIDROIT Principles of International Commercial contracts, 1994, published by the International Institute for the Unification of Private Law (UNIDROIT), Rome, Italy, may be viewed at the following web address: http://www.jus.uio.no/lm/unidroit.contract.principles.1994/doc.html, last visited 31.08.2001.

than another more appropriate user. There should thus also be a clause providing that the system operators are not responsible for the accuracy or otherwise of the data furnished to the integration tool (e.g. upon registration) and that the responsibility for such data remains solely with the person who furnished it (e.g. see sample Clause 9 in Appendix 4).

In commercial contracts, it is common to try to limit liability up to the amount paid/earned on the contract by the party who suffered damages (e.g. the contract price). Once it has been determined how the MEIT MSP is going to generate income through the tool, (e.g. through an annual subscription fee), one could use this to calculate and insert a cap on the MSP's liability through a clause such as, for example, draft Clause 14(2).

Moreover, one should also consider having a limitation on consequential, special, incidental and indirect damages to limit the MEIT MSP's exposure to open-ended liability. Such a limitation clause is another common provision in commercial transactions. (See draft Clause 14(1) in Appendix 4.)

4.6.3 Liability of the system developer

The draft clause in the MEIT User agreement attempts to delimit the liability of the MSP towards the MEIT user, since such agreement is between the user and the MSP. However, one could envisage the possibility of a claim for liability by the MSP against the MEIT system developer (where this is developed into a commercial product by an entity other than the MSP). This matter should be regulated through a liability clause in the system development contract between the MSP and the system developer.[144] The alleged defect or malfunction should be examined on its particular merits and circumstances, and it is difficult to guess beforehand what the consequences will be. It might therefore be advisable for, respectively, the MEIT MSP and the system developer, to seek additional cover (besides the limitation of liability clause) by taking up liability insurance against any potential claims made for malfunction of the system.

144. As regards the liability - if at all - of the system contributors (i.e. the domain experts), this has been discussed in literature, with such persons being called "Almost Untouchables" on the basis that public policy considerations would result in restrictions being placed upon regular negligence liability, "although gross negligence and intentional torts will probably remain actionable. The idea is that the public interest in acquiring and preserving the experts' propositional and heuristic knowledge would afford scope for encouraging contributions to such expert systems. Willick, M.S., *Professional Malpractice and the Unauthorized Practice of Professions: Some Legal and Ethical Aspects of the Use of Computers on Decision-Aids*, 1986, quoted by Cannataci J.A, in *Liability and responsibility for expert systems*, Complex 5/88, Tano, 1988, at p. 48.

Finally, it should perhaps also be mentioned that the fact that the users of the MEIT are intended to be commercial entities and not private persons has the consequence of excluding the applicability of the EU Product Liability Directive[145] since this is limited to damage[146] suffered by consumers.[147]

145. Council Directive EC/85/374 on Liability for Defective Products, 25.07.1985, O.J. L 210, 07/08/1985 pp. 0029 – 0033, also available at http://europa.eu.int/eur-lex/en/lif/dat/1985/en_385L0374.html, last visited 15.08.2001.
146. See Article 9 of the Product Liability Directive, *supra* n. 134.
147. This Directive covers both damage caused by death or personal injury, and also "damage to or destruction of, any item of property other than the defective product itself, with a lower threshold of 500 EURO, provided that the item of property: (i) is of a type ordinarily intended for private use or consumption, and (ii) was used by the injured person mainly for his own private use of consumption." For more discussion on the Product Liability Directive, see Stapleton J, *Product Liability*,1994, Butterworths, p. 280 and Kelly, P. & Attree, R., *European Product Liabilities*, Butterworths, 1997.

5. CONTRACTING AMONG THE VIRTUAL ENTERPRISE PARTNERS: SPECIAL MARITIME CONTRACTS

5.1 Introduction

As described in the life-cycle of the virtual enterprise in Chapter 2, once the need for the creation of virtual enterprise has been identified, there is then a search for the partners with the required core competencies to come together to form the virtual enterprise. This is followed by contract negotiation and signature between the members of the virtual organisation and the customer.

However, in the field of emergency repair and planned maintenance, there are certain domain-specific peculiarities which limit the partner search. This is because a partner may already be pre-determined (e.g. the classification society, the Emergency-Response Company) through pre-existing contractual agreements with the customer of the virtual enterprise (i.e. the shipowner or ship manager). Therefore, naturally, there is no need for further contracts to be signed between such actors.

Nevertheless, there are other partners with whom there will be no pre-existing contractual relationship, e.g. tug company or shipyard to repair the vessel, and here the partner search and electronic contracting (phases 2 and 3 in the life-cycle of the virtual enterprise described in Section 2.1) become relevant. Once such an actor, such as a shipyard, has been selected to carry out the repair of the ship following an emergency or because of planned maintenance, there is a process of tendering, contract negotiation and agreement with regards to the repair contract.

5.2 Electronic contracting between the virtual enterprise partners

A possible feature of the MEIT could be a facility which allows the parties to select and agree on the terms and conditions which are to govern such agreements (i.e. towing and ship repair). In the case of towage and salvage, this process can be facilitated because of the existence of a number of standard contracts in this field. Contracting could be done electronically between the parties, and reference is made to Section 4.2 in this study on web contracting. In fact, much of the contracting and sub-contracting in the maritime industry

is done through the use of standard form agreements that have been developed by maritime associations such as Lloyds of London.

For example, in salvage, the Lloyd's Standard Form of Salvage Agreement (the Lloyd's Open Form or "LOF") is generally used.[148] This form was originally published in 1908 and is now in its tenth revision with the LOF 2000,[149] though previous editions of the form, i.e. the LOF 1995, LOF 1990 and LOF 1980 are still in use today. It has been reported that on average, the Lloyd's Open Form is used in 150 salvage incidents each year. In 1999, over £16 million in payments were made as a result of the form's use.[150] There is also a BIMCO[151] "Salvhire" and "Salvcon" form which is in use in salvage when engaging tugs and equipment on a daily or lump sum basis.

In towage, there are a number of standard form contracts that have been developed by tug owners' associations such as the U.K. Standard Conditions for Towage and Other Services,[152] BIMCO's "Towhire" and "Towcon" forms of 1985 supplemented by the "Supplytime 89", the Netherlands Tug Owners Conditions 1951,[153] the Scandinavian Tugowners' Standard Conditions 1959 (1974 Revision).[154] Some tug operators have developed their own in-house forms.[155] Some of these standard forms provide a space for the signature of the

148. The fundamental principle under which the LOF operates, apart from one notable exception (special compensation) is that of "no cure – no pay". That is, if a salvor engaged to conduct services under the LOF is unsuccessful in its attempts to salve a ship and/or cargo then it gets no reward despite the fact that it may well have expended a significant amount of resources in endeavouring to achieve success. On the other hand, if it was successful, it could hope for a fair reward. A panel or arbitrators, barristers specialising in Admiralty law, are retained by Lloyd's to hear cases which arise under the agreement and to produce salvage awards.
149. A copy of the LOF 2000 may be downloaded from Lloyd's web sit at the following address: http://www.lloydsoflondon.com/agencysalvage/salvage/theform/body.htm, last visited 31.08.2001.
150. See Lloyd's website at http://www.lloydsoflondon.com/agencysalvage/salvage/launch/body.htm, last visited 31.08.2001.
151. Baltic and International Maritime Council.
152. This form, produced by the British Tugowners' Association, is used for port and harbour work as well as some offshore work – see Rainey, Simon, *The Law of Tug and Tow*, 1996, LLP, p. 7.
153. Towage in Dutch territorial waters by a Dutch tug owner is subject to the Netherlands Tug Owners Conditions unless otherwise stipulated expressly and in writing; outside the Netherlands the Conditions have to be expressly incorporated into the contract in order to bind the owner of the tow.
154. If it is decided to try and include a copy of a number of these standard contracts in the MEIT, permission should first be sought from the relevant entity (e.g. tug owner association) that owns the rights to such standard contract.
155. See Rainey, S., supra n. 152., p. 7.

Tug owner and the Hirer (e.g. the BIMCO forms) whereas others are standard conditions which could be incorporated into an agreement between the parties.

Today it is already the case that some of these standard contracts may be agreed to orally or via radio. For example, the Lloyds LOF 1995 may be agreed to either orally or via radio through sending the following message:

> *"Accept salvage services on basis Lloyd's Standard Form LOF 1995 - no cure no pay - Acknowledge repeating foregoing. Master …"*[156]

Such agreement might be mirrored electronically, with electronic messages such as e-mail being transmitted between the parties instead of radio messages.[157]

It is to be borne in mind that the constitutive element of a contract is the agreement between the contracting parties (with a minimum of at least two parties) on the terms of a contract. This agreement usually takes the form of an offer and an acceptance which matches the offer, both of which can be transmitted electronically. A difficulty that might arise in this context, where such messages are transmitted electronically such as via e-mail, is that not all legal systems have the same rules as to the moment that a contract is deemed to have been concluded. Some countries require that the acceptance should have left the system of the acceptor, others require that it should have been received by the offeror, while others still require that the offeror should have knowledge of the acceptance. It is therefore perhaps advisable to have a clause in the MEIT Agreement whereby the Users agree on when a contract (concluded via the MEIT system) is deemed to have been concluded. An example of such clause would be draft Clause 10(3) which is based on Article 3.3 of the European Model Electronic Data Interchange Agreement,[158] for example:

> *"You agree that a contract effected between you and another or other Users by use of the System shall be concluded at the time and place where the message constituting the acceptance of an offer reaches the computer system of the offeror. You undertake and bind yourself to include a clause in any and all electronic agreements that you may enter into with any other User or Users of this System whereby you expressly agree that a*

156. See Section 6.2.2, *op. cit.* at n. 5.
157. A difference between radio and Internet communication is that the former is a one-to-many communication and is usually on a specific bandwidth, whereas Internet communication in this example would be a one-to-one communication between the ship crew or ship manager and the salvage company.
158. For further reading on this point, see Davies, L. S. '*Contract Formation on the Internet (Shattering a Few Myths)*', in 'Law and the Internet', 1997, Hart Publishing, Oxford.

contract effected between you and such other User or Users shall be deemed to have been concluded at the time and place where the message constituting the acceptance of an offer reaches the computer system of the offeror."

Suffice it to say that it would perhaps be wise to request an acknowledgement of the acceptance message and, indeed, to make the acceptance conditional upon the receipt of an acknowledgement within a specified time limit.

Where there is a statutory requirement that a signature should be hand written, a problem arises since this could constitute an obstacle to an agreement on the application of a standard contract being entered into between the parties via the Internet (through electronic signature). Other constraints are legislative controls on the use of digital signature. However, where a standard form may be incorporated into an agreement by reference, then there should be no obstacles to the agreement being concluded electronically.

Where there exist no standard form contracts on a particular matter or where the parties (who, of course, may be two or more) opt to negotiate on the basis of an in-house contract instead, then the drafts of such a contract can be exchanged electronically (e.g. as e-mail attachments) between the parties, with each partner having the facility of proposing amendments to certain contractual clauses and then circulating it to the other parties, until eventually all the parties have agreed to all the contractual terms.

6. CONCLUDING REMARKS

As explained in the Introduction, this study is based on a report drawn up in the MARVIN project which sought to provide a practical legal framework for the operation of the maritime virtual organisation.[159] It focuses on issues which are relevant both during an emergency repair and a planned maintenance situation. However, a number of the legal issues discussed are relevant to other types of virtual organisations in other domains.

This study commenced with an analysis of the legal nature of the virtual organisation, and of the possible legal and business structures that may be used for such organisations. This was followed by a look at different aspects and features of the integration tool, and the relationship between the users themselves upon the creation of a virtual organisation.

The focus was then shifted to the legal issues that arise from the use of the integration tool by the users for the transmission of information. A problem arises where a request is made for the transmission of certain ship information that is protected from disclosure to third parties by confidentiality clauses or under intellectual property law. The holder of the information usually insists on the receipt of a consent in writing from the owner of the sensitive information. It is concluded in this study that at least equivalent reassurance of the authenticity and integrity of the consent is given where such message is encrypted and accompanied by a digital signature. Moreover, the extent to which encryption and digital signature technology could be used to address security and authentication concerns was examined, with a look at some existing controls on the export and domestic use of encryption software.

The elements of a framework agreement - the MEIT User Agreement - to be entered into by every user of the MEIT upon registering with the system have also been outlined, and a number of draft clauses for such an agreement are proposed.[160] This User Agreement should cover thorny legal issues such as formation and validity of electronic contracts, the extent to which such contracts are admissible as evidence, choice of law and forum, and liability for defects of the integration tool. It is proposed that there should be an explicit or express choice of law and jurisdiction clause in the MEIT User Agreement.

---

159. See *supra* n. 5.
160. See, in particular, Appendix 4 of this study.

Finally, the contractual relationship between the partners selected to form the virtual enterprise and their client is examined. In the maritime field, one often finds a number of standard maritime contracts in use. A possible feature of the MEIT is suggested to allow the parties to select the particular (and sometimes standard form) contract which is to be used for certain maritime operations such as salvage and/or towing.

The focus of the MARVIN report, on which this study is based, is on maritime virtual organisations. However, an attempt is made in this study to also address general legal issues related to virtual organisations that will hopefully be of relevance to virtual organisations in other business domains.

TABLE OF STATUTES, CONVENTIONS AND INSTRUMENTS

Conventions

Convention on the Law Applicable to International Sale of Goods, The Hague, 1955, available at http://www.ulcc.ca/en/us/?sec=1&sub=1l&print=1#2, last visited 31.08.2001.

EC Convention on Jurisdiction and the Enforcement of Judgments in Civil and Commercial Matters, Brussels 1968 (Full Faith and Credit Convention), O.J. L 299, 31/12/1972, pp. 0032 – 0042, also available at http://europa.eu.int/eur-lex/en/lif/dat/1968/en_468A0927_01.html, last visited 31.08.2001.

EC Convention on the Law Applicable to Contractual Obligations (Rome 1980), O.J. C 027, 26/01/1998, pp. 0034 – 0046, also available at http://www.jus.uio.no/lm/ec.applicable.law.contracts.1980/doc.html, last visited 31.08.2001.

1988 Lugano Convention on Jurisdiction and the Enforcement of judgments in Civil and Commercial Matters, O.J. No. L 319 , 25/11/1988, pp. 0009 – 0033, also available at http://europa.eu.int/eur-lex/en/lif/dat/1988/en_488A0592.html, last visited 31.08.2001.

European Union

Directives

Council Directive EC/85/374 on Liability for Defective Products, 25.07.1985, O.J. L 210, 07/08/1985 pp. 0029 – 0033, also available at http://europa.eu.int/eur-lex/en/lif/dat/1985/en_385L0374.html, last visited 15.08.2001.

Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and the free movement of such data, O.J. L 281 p.31, 23/11/1995.

Directive 97/7/EC of the European Parliament and of the Council of 20 May 1997 on the protection of consumers in respect of distance contracts, O.J. L 144, 04/06/1997, pp. 0019 - 0027.

Directive 97/36/EC of the European Parliament and of the Council of 30 June 1997 amending Council Directive 89/552/EEC on the coordination of certain provisions laid down by law, regulation or administrative action in Member States concerning the pursuit of television broadcasting activities, O.J. L 202 p. 60, 30/07/1997.

Directive 1999/93/EC of the European Parliament and of the Council of 13 December 1999 on a Community framework for electronic signatures, O.J. L 13, 19.01.2000, p. 12, available at http://europa.eu.int/eur-lex/en/lif/dat/2000/en_300L0031.html, last visited 31.08.2001.

Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market, O.J. L 178, 17.7.2000, also available at http://europa.eu.int/eur-lex/en/lif/dat/2000/en_300L0031.html, last visited 15.08.2001.

Recommendations

94/820/EC: Commission Recommendation of 19 October 1994 relating to the legal aspects of electronic data interchange (Text with EEA relevance), O.J. L 338 , 28/12/1994. pp. 0098 – 0117.

Regulations

Council Regulation (EC) No 3381/94 of 19 December 1994 setting up a Community regime for the control of exports of dual-use goods, O.J. L 367, 31.12.1994, pp. 0001-0007 – Regulation as amended by Regulation No. 837/95, O.J. L 90, 21.04.1995, pp. 0001-0007.

Council Regulation No. 1334/2000 setting up a Community regime for the control of exports of dual-use items and technology, O.J. L 159, 30.06.2000, pp. 0001-0215.

Council Regulation (EC) No 458/2001 of 6 March 2001 amending Regulation (EC) No 1334/2000 with regard to the list of controlled dual-use items and technology when exported, O.J. L 065, 07/03/2001, pp. 0019-0019.

Council Regulation (EC) No 44/2001 of 22 December 2000 on jurisdiction and the recognition and enforcement of judgments in civil and commercial matters, O.J. L 012, 16/01/2001, pp. 0001 – 0023.

Germany

Bürgerliches Gesetzbuch (Civil Code), § 141, 272, 276, 278.

Greece
Civil Code, Article 332

Ireland
Electronic Commerce Act 2000.

Portugal
Civil Code, Articles 800, 809.

Norway
Lov om elektronisk signatur 15. Juni 2001 nr. 81.

Spain
General Telecommunications Law of 24 April 1998.

United Kingdom
Regulation of Investigatory Powers Act 2000.

Miscellaneous
UNCITRAL Model Law on Electronic Commerce, 1996, available at http://www.jus.uio.no/lm/un.electronic.commerce.model.law.1996/doc.html, last visited 31.08.2001.

Wassenaar Arrangement on Export Controls for Conventional Arms and Dual-Use Goods and Technologies, 1996, http://www.wassenaar.org, last visited 31.08.2001.

BIBLIOGRAPHY

Angeli R., (ed.) *Final Virtual Organisation Architecture*, MARVIN Deliverable No. T1.3D2, November 2000.

Angeli R., Odendahl C., Kraus S., *Final Specification of Software and Interfaces*, MARVIN Deliverable No. T3.1D2 (restricted), June 2000.

Baker, S.A. & Hurst, P.R., *The Limits of Trust: Cryptography, Governments, and Electronic Commerce*, 1998, Kluwer Law International.

Beale, H.G. (ed.), *Chitty on Contracts*, Vol. 1 General Principles, 28th ed., Sweet & Maxwell, London, 1999.

Berwanger, E., "The Legal Classification of Virtual Corporation According to German Law", in *Organizational Virtualness and Electronic Commerce: Proceedings of the 2nd International VoNet Workshop, September 23-24, 1999,* Simowa Verlag Bern.

Brazell, L., Encryption Security: Encryption in the Real World, [1999] *European Intellectual Property Review* 17.

Brækhus, S., *Choice of Law Problems in International Shipping (Recent Developments)*, 1980, Sijthoff & Noordhoff.

Bundesausfuhramt - German Federal Export Office, BAFA *Exportkontrolle – Kurzdarstellung*, 1st November 2000 edition, online at http://www.bundesausfuhramt.de.

Burnstein, M., "A Global Network in a Compartmentalised Legal Environment", *Internet: Which Court Decides? Which Law Applies? Quel tribunal décide? Quel droit s'applique?*, Boele-Woelki & Kessedjian eds., 1998, Kluwer Law International.

Cannataci, J.A, *Liability and responsibility for expert systems*, Complex 5/88, Tano, 1988.

Curtis, S., *The Law of Shipbuilding Contracts*. 2nd ed., 1996, LLP.

Davies, L.S. *'Contract Formation on the Internet (Shattering a Few Myths)'*, in 'Law and the Internet', 1997, Hart Publishing, Oxford.

Gaskell, N.J.J., Debattista, C., & Swatton, R.J., *Chorley & Giles' Shipping Law*, 8th ed., 1987, Pitman Publishing.

Goldrein, I., (ed.), *Ship sale and purchase*, 3rd ed., 1998, LLP.

Greguras, F.M., Golobic, T.A., Mesa, R.A. and Duncan, R., *Electronic Commerce: On-line Contract Issues* at the following web site address http://www.armyec.sra.com/knowbase/docs/doc121/ec_contr.html.

Haenisch, J. (ed.) *Final user requirements and models (business processes)*, MARVIN Deliverable No. T1.1D2, December 2000.

Hill, C., *Maritime Law*, 5th ed., 1998, LLP.

Holland, C.P., "The importance of Trust and Business Relationships in the Formation of Virtual Organisations", in *Organizational Virtualness: Proceedings of the VoNet Workshop, April 27-28, 1998*, 1998, Simowa Verlag Bern.

Jansen, W., Steenbakkers W. and Jägers, H. "Electronic Commerce and Virtual Organizations", in *Organizational Virtualness and Electronic Commerce: Proceedings of the 2nd International VoNet Workshop, September 23-24, 1999*, Simowa Verlag Bern.

Jaramillo, D. (ed.), *Final User Requirements and Models (business information and product data)*, MARVIN Deliverable No. T1.2D2, January 2001.

Jägers H, Jansen W., Steenbakkers W., "Characteristics of Virtual Organizations", in *Organizational Virtualness: Proceedings of the VoNet Workshop, April 27-28, 1998*, 1998, Simowa Verlag Bern.

Kelly, P. & Attree, R., *European Product Liabilities*, Butterworths.

Kennedy, G., "Encryption Policies: Codemakers, codebreakers and rulemakers: Dilemmas in current encryption policies", [2000] *CLSR* Vol. 16 no. 4.

Kronke, H., "Applicable Law in Torts and Contracts in Cyberspace", *Internet: Which Court Decides? Which Law Applies? Quel tribunal décide? Quel droit s'applique?*, Boele-Woelki & Kessedjian eds., 1998, Kluwer Law International.

Kuner, C., *Proposed Amendments to the German Digital Signature Law*, http://www.kuner.com.

Lando, O. & Beale, H., *The Principles of European Contract Law*, 1995, Martinus Nijhoff Publishers.

Makris, S., (ed.), *Validation of prototypes*, MARVIN Deliverable No. T4.1D1, (restricted), June 2000.

Mertens, P., Faisst, W., "Virtuelle Unternehmen - Idee, Informationsverarbeitung, Illusion", in "Scheer, A.-W. "Organisationsstruckturen und Informationssysteme auf dem Prüfstand", 18. Saarbrücker Arbeitstagung 1997, Heidelberg 1997.

Odendahl, C.; Reimer, S.; Marzen, S., "Fallstudie zum Projekt 'Konzeption und Entwicklung einer Kooperationsbörse zur kontinuierlichen Gestaltng Virtueller Unternehmen", Bibliothek der Kooperationsbörse, http://www.iwi.uni-sb.de/research/index_e.htm, last visited 31.08.2001.

Odendahl, C.; Scheer, A.-W., "The Concept of Virtual Enterprises and ist Relevance for the Maritime Domain", in Guedes Soares, C; Brodda, J. (Eds.), *Application of Information Technologies to the Maritime Industries*, Edições Salamandra, Lisbon, 1999, pp. 11-31.

OECD Group of Experts on Information Security and Privacy, *Inventory of Controls on Cryptography Technologies*, Directorate for Science Technology and Industry, Committee for Information, Computer and Communications Policy, 24 September 1998, DSTI/ICCP/REG(98)4/REV3.

OECD Group of Experts on Information Security and Privacy, *Inventory of Approaches to Authentication and Certification in a Global Networked Society*, Directorate for Science Technology and Industry, Committee for Information, Computer and Communications Policy, 4th October 1999, DSTI/ICCP/REG(99)13/FINAL.

Pletsch, A. "Organizational Virtualness in Business and Legal Reality", in *Organizational Virtualness: Proceedings of the VoNet Workshop, April 27-28, 1998,* 1998, Simowa Verlag Bern.

Racicot, M., Hayes, M.S., Szibbo, A.R. & Trudel, P., *The Cyberspace is Not a "No Law Land" - A study of the Issues of Liability for Content Circulating on the Internet*, prepared for Industry Canada, 1997, issued also on Internet http://www.strategis.ic.gc.ca/nme.

Rainey, S., *The Law of Tug and Tow*, 1996, LLP.

Stapleton, J, *Product Liability*,1994, Butterworths.

Tetley, W., *International Conflict of Laws: Common, Civil and Maritime*, 1994, International Shipping Publications.

Weitzenböck, E., *Final legal framework for the maritime virtual organisation*, MARVIN Deliverable No. T1.4D2, November 2000.

Wyatt & Dashwood's European Community Law, 3rd ed., London, Sweet & Maxwell, 1993.

APPENDICES

Appendix 1: Extract from the MARVIN Project Programme

3.2.2.1.4 Task 1.4: Legal framework for virtual organisations (IRI)

Objectives:

1. To establish a legal framework, in the interest of both users and the partners who will supply services to them, for operating a virtual maritime organisation.

Approach: Much of the contracting and sub-contracting in the maritime industry is done using standard contracts which may need to be reviewed in the light of the specific virtual environment of the proposed software tool. The task will, therefore, focus on providing a framework agreement/legal environment for the software tool, in particular with regards to the two proposed scenarios. This will include an examination of the legal issues, which arise from operating the virtual organisation on the Internet such as: legal safeguards on intellectual property matters (e.g. protection of design drawings of ship components, etc.); confidentiality of commercially sensitive data - this may include an examination of legality of encryption techniques for message transfer; limitation of liability of the partners who supply the services; jurisdiction or arbitration clause; an underlying interchange agreement between all parties involved concerning the agreed electronic data interchange (EDI) message standard and protocols to be applied, and the procedure of confirmation, authentication and security of the EDI messages (including use of encryption techniques). Requirements from the technical development will be used as input.

The framework will be validated by the project user group (this group includes yards, ship management company and classification societies) using the prototype and the two validation scenarios. The results of this validation will be used to refine the framework."

Appendix 2: Extract from the MARAD form

Article V: Rights of purchaser and board with respect to engineering and design data

"(a)All design and engineering data furnished to the Contractor by the Purchaser or the [U.S. Maritime Subsidy] Board which are the property of the Purchaser or the Board shall remain the property of the Purchaser and the Board as their interests appear. The use or reuse of said design and engineering data by Contractor shall be governed by the Purchaser and the Board as their interests appear.

(b) All plans, including working plans (including reproducibles) and such other specified design and engineering data required to be furnished to the Purchaser by the Plans and Specifications and produced by the Contractor in the performance of this Contract, shall be the sole property of the Purchaser and the Board as their interests appear and the Purchaser or the Board shall have the full right to use the same in such manner as each may deem proper, including without limitation to the generality of the foregoing, the right to make reproducibles and copies, the right to publish, or to withhold from publication and the right to make alterations therein, additions thereto, or other changes. Except as provided in Article 7 of Contract MA/MSB- ....., the Contractor shall be entitled to recover the reasonable costs of reproduction and handling in the event that the Contractor is required by the Purchaser or the Board to provide copies of such plans, working plans and design and engineering data to the Board, the Purchaser or any designee of the Board or Purchaser. Unless prohibited by provision of law relating to the National Defence or security, the Contractor shall be permitted to retain copies or duplicates of such plans, working plans and design and engineering data for its own official records. The Contractor shall have the right with the approval of the Board to construct a ship or ships built to such plans, working plans and design and engineering data and the Contractor shall have the right with the approval of the Board to transfer such plans, working plans and design and engineering data provided that neither Purchaser nor Contractor shall be entitled to any fees, commissions or other monetary benefits (except the reasonable costs of reproduction and handling) for such use or transfer.

(c) All design and engineering data, plans and working plans furnished by the Contractor in the performance of this Contract but which were not produced by Contractor in the performance of this Contract shall not become the property of the Purchaser or the Board; provided, however, that the Contractor shall commit to the Board that the Contractor will make such

design and engineering data, plans and working plans available to any party that the Board may from time to time designate in return for the payment by the designated party of a reasonable royalty, license fee or commission. The Contractor's commitment shall apply to both patented and unpatented design and engineering data, plans and working plans, but shall not apply to design and engineering data, plans and working plans licensed by the Contractor from an unaffiliated third party where the terms of the license prevent such a commitment by the Contractor.

(d) Unless otherwise directed by the Board or the Purchaser, the Contractor shall take reasonable precautions to maintain in confidence all information contained in the Plans and Specifications disclosed to it other than information which is known to it at the time of such disclosures, or which is or shall become available to it from sources other than the Purchaser, the Board, or the Naval Architect of the Purchaser, or which is or shall become obvious to those skilled in the trade to which such information relates. Notwithstanding anything to the contrary hereinabove contained, the Contractor shall not be precluded from disclosing information which may be necessary for the prosecution of the contract work, provided only that in making such disclosure the Contractor shall impose upon any person, firm or corporation to whom such disclosure is made, conditions relating to the confidential treatment thereof to the same effect as those imposed upon it herein; nor shall the Contractor be responsible for unauthorized actions of its employees provided that the aforementioned reasonable precautions have been taken by it as hereinabove provided."

Appendix 3: Extract from the EU Dual-Use Regulation

General Technology Note

(To be read in conjunction with section E of Categories 1 to 9.)

The export of "technology" which is "required" for the "development", "production" or "use" of goods controlled in Categories 1 to 9, is controlled according to the provisions of Categories 1 to 9.

"Technology" "required" for the "development", "production" or "use" of goods under control remains under control even when applicable to non-controlled goods.

Controls do not apply to that "technology" which is the minimum necessary for the installation, operation, maintenance (checking) and repair of those goods which are not controlled or whose export has been authorised.

N.B.:This does not release such "technology" specified in 1E002.e. and 1E002.f., 8E002.a. and 8E002.b.

Controls on "technology" transfer do not apply to information "in the public domain", to "basic scientific research" or to the minimum necessary information for patent applications.

General Software Note

(This note overrides any control within section D of Categories 0 to 9)

Categories 0 to 9 of this list do not control "software" which is either:

a. Generally available to the public by being:

   1. Sold from stock at retail selling points, without restriction, by means of:

      a. Over-the-counter transactions;

      b.Mail order transactions; or

      c.Telephone order transactions; and

   2. Designed for installation by the user without further substantial support by the supplier; or

   N.B. Entry a. of the General Software Note does not release "software" specified in Category 5 - Part 2 ("Information Security").

b. "In the public domain".

Appendix 4: Sample clauses for a MEIT User Agreement

NB: This part is to be read in conjunction with Chapter 4.

1. Acceptance of Terms & Duration

(1) We, [*the MSP*][161] offer our Service to you subject to the terms and conditions of this Agreement. By clicking on the button marked "I Agree" appearing on the screen immediately at the end of these terms and conditions, you are deemed to have accepted our Service and agreed to be bound by and to comply with, the terms and conditions of this Agreement.

(2) This Agreement shall continue until terminated by you or us giving the other at least fifteen days' written notice of termination, such termination to be effective upon the expiry of the aforesaid period of notice.

2. Definitions

In this Agreement:

Agreement means this agreement and the Technical Annex thereto[162] for the provision of Services between you and us;

Commercial Communication is any form of communication designed to promote, directly or indirectly, the goods, services or image of a company, organisation or person pursuing a commercial, industrial or craft activity or exercising a regulated profession;

Provided that the following do not in themselves constitute commercial communications:

(i) information allowing direct access to the activity of the company, organisation or person, in particular a domain name or an electronic-mail address,

(ii) communications relating to the goods, services or image of the company, organisation or person compiled in an independent manner, particularly when this is without financial consideration."

Content has the meaning set out in Clause 9;

---

161. This should, of course, contain the correct name of the MSP.
162. See *supra* Section 4.3. Note that the terms and conditions of this Technical Annex should be follow immediately after the end of the text of the agreement and the User should be compelled to scroll through the Technical Annex as well.

Counterparty Data means data of any kind sent or made available to you using the System (including such data subsequently stored on equipment or other hardware devices owned or controlled by you) including, but not limited to voice, graphics, sound, video and text data;

Customer Data means data of any kind that you enter into the System, including but not limited to voice, graphics, sound, video and text data;

Data means Customer Data or Counterparty Data or both;

Data Message means information generated, sent, received or stored by electronic, optical or similar means, including but not limited to, electronic mail or telefax;

Data Store means devices for the storage of Data operated by us including, but not limited to hard disc drives, optical disc drives (including CD Rom drives), memory devices of all types, floppy disc drives and all other devices capable of storing data on magnetic or other media;

Service means the service provided by us under this Agreement of any of the following:

(a) the sending, receiving, storage, processing or other communication of Data;

(b) the sorting, processing and/or shortlisting of potential Users who may offer the services and/or products that you are seeking through this Service.

Software means any software in which we own or co-own intellectual property rights (other than third party software which we use under licence) which is operated by access to the Website or provided to you for installation on equipment or other devices owned or controlled by you, and any modifications or enhancements thereto from time to time made accessible or (as the case may be) provided to you by us;

System means the Website, the Software and the Data Store;

we and **us** mean ……;[163]

Website means the website whose address is……;[164]

User means a user of the System;

---

163. Here the name of the MSP should be inserted.
164. Here the website of the MEIT system should be inserted.

you means the person, firm or company who has entered into this Agreement with us and includes any person, firm or company acting with apparent authority on your behalf.

3. Description of Service

(1) Unless explicitly stated otherwise, any new features that add to or enhance the current Service, shall also be subject to this Agreement.[165]

(2) In order to use these Services, you must obtain access to the World Wide Web either directly or through devices that access web-based content, and pay any service and/or telephony fees associated with such access. In addition, you must provide and pay for all equipment necessary to make such connection to the World Wide Web, including a computer and modem or other access device.

4. Registration Obligations

You agree to:

(a) provide true, accurate, current and complete information about yourself as prompted by the Service's registration form and other forms (such information being the "Registration Data") and

(b) maintain and promptly update the Registration Data to keep it true, accurate, current and complete. If you provide any information that is untrue, inaccurate, not current or incomplete, or we have reasonable grounds to suspect that such information is untrue, inaccurate, not current or incomplete, we have the right to suspend or terminate your account and refuse any and all current or future use of the Service (or any portion thereof), and if appropriate, take any legal action as may be pertinent at law.

5. User Account and Password

(1) Upon completion of the online registration process:

(a) you will be asked to choose a user password;

---

165. An alternative to this clause would perhaps be to have some sort of committee made up of representatives of different categories of registered Users of the MEIT (e.g. shipowners, shipyards, etc.) who would discuss and decide together with the MSP what enhancements and new features proposed to be made to the System should form part of the Agreement. This would mean that enhancements and new features would not automatically fall within this Agreement. It is very important to ensure that decisions can effectively be reached within this committee and that the members would not be deadlocked.

(b) we shall use our reasonable endeavours to supply you with a user name as soon as possible.

(2) We shall not be liable for any loss or damage caused by any delay in our supplying you with a user name.

(3) You are responsible for maintaining the confidentiality of the password and are fully responsible for all activities that occur under your password or account. You agree to:

(a) immediately notify us of any unauthorised use of your password or account or any other breach of security, and

(b) ensure that you exit from your account at the end of each session.

We cannot and will not be liable for any loss or damage arising from your failure to comply with this provision.

6. Variation of Agreement

Terms contained in this Agreement may be changed at our discretion provided that a minimum of four weeks' written notice is given by us to you.

7. Use of the service

(1) You agree that, in respect of all transactions in respect of which the System has been used at any stage (whether or not the transaction was concluded over the System), you will immediately notify us of any amount due in respect thereof.[166]

(2) You agree to maintain in strictest confidence all aspects of the Service and the System which are not already in the public domain or comprise the Data (the "Confidential Information") and that you shall not use for any purpose, nor disclose to any person, the Confidential Information save as is necessary for the proper performance of this Agreement.

(3) You agree to only use the Service for lawful purposes and also specifically agree that:

(a) you shall not (or authorise or permit any other party to) use the Service to receive or send any material which is in violation of any law or

166. This is to enable the commission to be calculated. We assume in this clause that a commission will be charged over gross value of the transactions made via the System – however, note that a business for exploitation of the METI system has not yet been developed and so this provision and Clause 19 merely serve to illustrate how a commission clause might be used.

regulation, which is obscene, threatening, offensive, defamatory, in breach of confidence, in breach of any property right (including copyright or other intellectual property right), or otherwise unlawful;

(b) impersonate any person or entity, falsely state or otherwise misrepresent your affiliation with a person or entity;

(c) you shall not knowingly or recklessly transmit any electronic material (including viruses) through the Service which shall cause or is likely to cause detriment or harm, in any degree, to computer systems owned by us or other Users.

(4) Commercial communication should comply with the following conditions:[167]

(a) the commercial communication shall be clearly identifiable as such;

(b) the natural or legal person on whose behalf the commercial communication is made shall be clearly identifiable;

(c) promotional offers are to be clearly identifiable as such.

8. Scope of the Service

(1) We are not a party to any transaction or proposed transaction between you and any other User and accordingly you accept that you will have no claim or cause of action whatsoever against us in respect of any such transaction or proposed transaction. You also accept that we are under no obligation to take any action to resolve any dispute between you and any other User, although if you notify us of a dispute we may, if we deem it appropriate, and in our sole option and discretion, investigate and consider assisting in the resolution of the dispute.

(2) We cannot guarantee that the Service will never be faulty, nor that it will work continuously, nor that it will be maintained in a fully operational condition or error free. However, we will use reasonable endeavours to correct serious faults reported by you as soon as we reasonably can. You undertake that if you become aware of a fault you will report it to us as soon as possible.

(3) Without prejudice to any other limitations or exclusions of our liability herein, including without limitation Clause 14, we shall have no liability whatsoever in respect of any failure on our part to repair a fault in the Service or to provide a continuous Service.

---

167. See Section 4.2.2 of this study.

9. Content

(1) You understand and agree that all information, data, text, software, music, sound, photographs, graphics, video, messages or other materials ("Content"), whether publicly posted or privately transmitted, are the sole responsibility of the person from which such Content originated. We do not guarantee or warrant the integrity, accuracy, legality or quality of any Content transmitted through our System.

(2) We shall not be held responsible or liable in any way for any Content, including but not limited to, for any errors or omissions in any Content, or for any loss or damage of any kind incurred as a result of the use of any Content posted, e-mailed or otherwise transmitted via the Service.

10. Legal validity and formation of electronic contracts

(1) You agree to be legally bound by the terms of this Agreement and expressly waive any rights to contest the validity this Agreement or of any other contract effected through this Service with any other User of this System on the sole ground that it was effected electronically.

(2) You undertake and bind yourself to include a clause in any and all electronic agreements that you may enter into with any other User or Users of this System whereby you expressly waive any right to contest the validity of such electronic agreement on the sole ground that it was effected electronically.[168]

(3) You agree that a contract effected between you and another or other Users by use of the System shall be concluded at the time and place where the message constituting the acceptance of an offer reaches the computer system of the offeror. You undertake and bind yourself to include a clause in any and all electronic agreements that you may enter into with any other User or Users of this System whereby you expressly agree that a contract effected between you and such other User or Users shall be deemed to have been concluded at the time and place where the message constituting the acceptance of an offer reaches the computer system of the offeror.[169]

---

168. See the discussion in Section 4.3 of this study.
169. Draft clause 10(3) is loosely based on Article 3.3 of the European Model Electronic Data Interchange Agreement. The second sentence is included to try to obviate arguments that the first sentence of this sub-clause is only enforceable by the MSP and the particular User but not by other User between themselves.

11. Equivalence of Data Message

Where any action is required by any Users of the System to be carried out in writing or by using a paper document, either between the Users and the System or between the Users themselves, such requirement is met if the action is carried out by using one or more Data Messages.[170]

12. Software

(1) You acknowledge and agree that the Service and the Software used in connection with the Service contain proprietary and confidential information that is protected by applicable intellectual property and other laws. You further acknowledge and agree that Content contained in information presented to you through the Service is protected by copyrights, trade marks, service marks, patents or other proprietary rights and laws. You agree not to adapt, modify, rent, lease, loan, sell, distribute the Software or create derivative works based on the Service or the Software, in whole or in part.

(2) We grant you a personal, non-transferable and non-exclusive right and license to use and copy the object code of our Software as is necessary for the performance of this Agreement.

13. Indemnity

The Service is supplied to you by us on the express condition that you do not use or intend to use the Service for any unlawful purpose and you agree to indemnify and hold us harmless from any claim, loss, demand, costs, expenses (including legal costs and expenses), fines or other liability whatsoever arising from any such unlawful use by you including (without limitation) liability arising out of any action brought against us for libel, slander, breaching data protection legislation or regulations, or infringement of copyright or any other intellectual property rights.

14. Limitation of Liability

(1) We shall be under no liability whatsoever for any loss, damage or injury including any direct, indirect, consequential or incidental loss or damage whatsoever suffered by you in the event that:

(a) you fail to keep confidential the user name and user password;

---

170. See Sections 3.1.3 and 4.3. This clause can be further qualified to apply where the data message is sent in a secure format.

(b) the loss or damage is caused by any breach by you of any of your obligations under this Agreement;

(c) the loss or damage is caused by the failure of any party with whom you have agreed a contract by use of the System to honour that contract in any respect, including without limitation contractual terms as to payment;[171]

(d) the performance of the Service by us is delayed, interrupted or otherwise prevented owing to events or conditions beyond our control including, without prejudice to the generality of the foregoing, storms, floods or other acts of God, the action of civil, military or governmental authorities, riots, civil commotion or strikes, acts of any government, power cuts, inability to obtain energy or suitable components, material, equipment or transportation, failure or non-operation of any telecommunications, telegraph and computer networks used by us (including without limitation the Internet and the World Wide Web) and the actions or neglect of any third party used by us to discharge its obligations under the Agreement including without limitation any domestic and international telecommunications and telegraph networks used in connection with the provision of the Service;

(e) the loss or damage is caused by our failure accurately to transmit, record or allow retrieval of recovery of any Data of any kind, or by the delay or total or partial failure on our part to perform the Service or any part thereof, unless in either case such failure arises from our gross negligence or wilful default in our performance of our obligations hereunder;

f) you fail to use or misuse the System, or because of your interpretation or misinterpretation of the results derived therefrom.

(2) Without prejudice to the foregoing our liability for any loss or damage arising directly or indirectly as a result of any breach of any express or implied term, condition, statement, warranty, undertaking or representation forming part of this Agreement or caused by any negligence, act, omission, mistake, interruption, delay, error or defect in the performance of the Service shall not exceed in respect of a claim or series of claims (whether related or unrelated) made by you in any period of twelve months the sum of ……..[172]

171. This seeks to safeguard the MEIT MSP from liability for loss/damage suffered by a User because of the failure of another User to honour its agreement with such User.

15. Suspension of Service

Without prejudice to any other right or remedy available to us, we shall be entitled without notice to you to suspend indefinitely the provision of the Service and of the User Name and User Password allocated to you in the event that:

(a) we have terminated the Agreement, such suspension to be effective at the end of the period of notice; or

(b) an event specified in Clause 13(d) occurs.

16. Notices

(1) Any notice or notification required to be given under or in connection with this Agreement shall be sent by registered mail or by a secure electronic mail[173] or, in the case only of a change in the terms of this Agreement by displaying an indication at the log-in page of the Website of the fact that there is to be a change to this Agreement and providing a link to a page detailing the change.

(2) Our address for service of notice shall be .....[174] or such other address of which we give you notice.

(3) Your address for service of notice shall be the address you enter online when entering into this Agreement or such other address of which you give us notice.

(4) Any such notice shall be deemed to have been served in the case of a notice:

(a) sent by registered post, at the expiry of 5 business days after it was posted;

(b) sent by electronic mail, at the time when the notice reaches the computer system of the party to whom or to which it has been sent if such time was during normal business hours, or at the beginning of the next business day in the place to which it was sent if such time was outside normal business hours.[175]

---

172. This should contain the cap on liability – see Section 4.6.
173. Technical specification of what is considered a secure electronic mail should be laid down in the Technical Annex to the agreement – e.g. a message that is certified by a Certification Service Provider.
174. The address and e-mail of the MSP should be inserted here.

17. General

(1) This Agreement represents the entire agreement between the parties in rela-tion to the provision of the Service and supersedes any previous agreement.

(2) You shall not assign or transfer the Agreement or any part of it or any of your rights, duties or obligations hereunder without our prior consent in writing. We may in our sole discretion assign or transfer this Agreement or any part of it.

(3) Any provision hereof which is void or unenforceable under the laws of…….[176] shall be to the extent of such invalidity or unenforceability deemed separable and shall not affect any other provision hereof.

(4) If we delay in acting upon a breach of this Agreement by you, then the delay shall not constitute a waiver by us of our rights and remedies in respect of the breach. If we do waive a breach of this Agreement, then that waiver is limited to that particular breach. The exercise of any one right or remedy in respect of a breach of this Agreement by us is without prejudice to any other rights or remedies we may have available.

18. Law and Jurisdiction

This Agreement and any other agreements between you and us shall be governed by the laws of ……..[177] and you and we hereby submit to the exclusive jurisdiction of the courts of ……..[178]

---

175. Where service is to be done by electronic mail, it is not easy to determine the time when such notice is to be deemed to have been served. Is it when it leaves the computer system of the sender, or when it is received by the addressee, or when the addressee actually reads it? Therefore it is suggested that the MEIT User Agreement should specifically state when service is deemed to have been made. Draft Clause 16(4)(b) is an example of such a clause, and has been loosely modelled on Article 3.3 of the European Model Electronic Data Interchange Agreement. Similarly, with regards to ordinary post – hence draft Clause 16(4)(a). See also see Section 5.2 of this study, with regards to a similar problem on the moment of conclusion of a contract.
176. The country whose law is chosen to be the governing law should be inserted here. See the comments in Sections 4.1 and 4.5 of this study and draft Clause 18.
177. The country whose law is chosen to be the governing law should be inserted here. See the comments in Sections 4.1 and 4.5.
178. The country which is chosen to be the forum should be inserted here. See the comments in Sections 4.1 and 4.5 of this study.

19. Charges

A commission of .....%[179] (..... per cent) shall be payable on the gross value of all transactions entered into over the System and shall fall due upon the last date that the invoice rendered therefor may be paid.[180]

179. This is a sample commission clause – see Section 4.1.
180. See comments in *supra* n. 166.

TIDLIGERE UTGITT I COMPLEX-SERIEN

CompLex er Institutt for rettsinformatikks skriftserie. Serien startet i 1981, og det har blitt utgitt mer enn hundre titler. Bøkene i CompLex-serien kan bestilles fra GnistAkademika (se bestillingsskjema bak i boken), eller lånes på biblioteket. CompLex-serien ligger i BIBSYS.

2001

1/01 **The International Sale of Digitised Products Through the Internet in a European Context**
Peter Lenda ..... *NOK 274.50*

2/01 **Internet Domain Names and Trademarks**
Tonje Røste Gulliksen ..... *NOK 227.-*

3/01 **Internasjonal jurisdiksjon ved elektronisk handel - med Lugano-konvensjonen art 5 (5) og elektroniske agenter som eksempel**
Joakim S. T. Øren ..... *NOK 204.-*

2000

1/00 **Klassikervernet i norsk åndsrett**
Anne Beth Lange ..... *NOK 268.-*

2/00 **Adgangen til å benytte personopplysninger. Med vekt på det opprinnelige behandlingsformålet som begrensningsfaktor**
Claude A. Lenth ..... *NOK 248.-*

3/00 **Innsyn i personopplysninger i elektroniske markedsplasser.**
Line Coll ..... *NOK 148.-*

1999

1/99 **International regulation and protection of Internet domain and trademarks**
Tonje Røste Gulliksen ..... *NOK 248.-*

2/99 **Betaling via Internett**
Camilla Julie Wollan ..... *NOK 268.-*

3/99 **Internett og jurisdiksjon**
Andreas Frølich Fuglesang & Georg Philip Krog ..... *NOK 198.-*

1998

1/98 **Fotografiske verk og fotografiske bilder, åndsverkloven § 1 og § 43 a**
Johan Krabbe-Knudsen ..... *NOK 198.-*

2/98 **Straffbar hacking, straffelovens § 145 annet ledd**
Guru Wanda Wanvik ..... *NOK 238.-*

3/98 **Interconnection - the obligation to interconnect telecommunications networks under EC law**
Katinka Mahieu ..... *NOK 198.-*

1997

1/97 **Eksemplarfremstilling av litterære verk til privat bruk**
Therese Steen ..... *NOK 158.-*

2/97 **Offentlige anskaffelser av informasjonsteknologi**
Camilla Sivesind Tokvam ..... *NOK 175.-*

3/97 **Rettslige spørsmål knyttet til Oppgaveregisteret**
Eiliv Berge Madsen ..... *NOK 170.-*

4/97 **Private pengespill på Internett**
Halvor Manshaus ..... *NOK 160.-*

5/97 **Normative Structures in Natural and Artificial Systems**
Christen Krogh.....*NOK 255.-*

6/97 **Rettslige aspekter ved digital kringkasting**
Jon Bing.....*NOK 178.-*

7/97 **Elektronisk informasjonsansvar**
Tomas Myrbostad.....*NOK148.-*

8/97 **Avtalelisens etter åndsverksloven § 36**
Ingrid Mauritzen.....*NOK 120.-*

9/97 **Krav til systemer for forvaltning av immaterielle rettigheter**
Svein Engebretsen.....*NOK 168.-*

10/97 **American Telephony: 120 Years on the Road to Full-blown Competition**
Jason A. Hoida.....*NOK 140.-*

11/97 **Rettslig vern av databaser**
Harald Chr Bjelke.....*NOK 358.-*

1996

1/96: **Innsynsrett i elektronisk post i offentlig forvaltning**
Knut Magnar Aanestad og Tormod S. Johansen.....*NOK 218.-*

2/96 **Public Policy and Legal regulation of the Information Market in the Digital Network Enviroment**
Stephen John Saxby.....*NOK 238.-*

3/96 **Opplysning på spill**
Ellen Lange.....*NOK 218.-*

4/96 **Personvern og overføring av personopplysninger til utlandet**
Eva I. E. Jarbekk.....*NOK 198.-*

5/96 **Fjernarbeid**
Henning Jakhelln.....*NOK 235.-*

6/96 **A Legal Advisory System Concerning Electronic Data Interchange within the European Community**
Andreas Mitrakas.....*NOK 128.-*

7/96 **Elektronisk publisering: Utvalgte rettslige aspekter**
Jon Bing og Ole E. Tokvam .....*NOK 186.-*

8/96 **Fjernsynsovervåking og personvern**
Finn-Øyvind H. Langfjell.....*NOK 138.-*

1995

1/95 **Rettslige konsekvenser av digitalisering: Rettighetsadministrasjon og redaktøransvar i digitale nett**
Jon Bing.....*NOK 368.-*

2/95 **Rettslige spørsmål i forbindelse med utvikling og bruk av standarder innen telekommunikasjon**
Sverre Sandvik .....*NOK 178.-*

3/95 **Legal Expert Systems: Discussion of Theoretical Assumptions**
Tina Smith .....*NOK 278.-*

4/95 **Personvern og straffeansvar - straffelovens § 390**
Ole Tokvam.....*NOK 198.-*

5/95 **Juridisk utredning om filmen «To mistenkelige personer»**
Johs. Andenæs .....*NOK 138.-*

6/95 **Public Administration and Information Technology**
Jon Bing and Dag Wiese Schartum.....*NOK 348.-*

7/95 **Law and Liberty in the Computer Age**
Vittorio Frosini .....*NOK 158.-*

1994

1/94 **Deon'94, Second International Workshop on Deontic Logic in Computer Science**
Andrew J. I. Jones & Mark Sergot (ed) .....*NOK 358.-*

2/94 **Film og videogramrett. TERESA (60)**
Beate Jacobsen .....*NOK 318.-*

3/94 **Elektronisk datutveksling i tollforvaltingen - Rettslige spørsmål knyttet til TVINN**
Rolf Risnæs.....*NOK 225.-*

4/94 **Sykepenger og personvern - Noen problemstillinger knyttet til behandlingen av sykepenger i Infotrygd**
Mari Bø Haugestad.....*NOK 148.-*

5/94 **EØS, medier og offentlighet. TERESA (103)**
Mads Andenæs, Rolf Høyer og Nils Risvand .....*NOK 148.-*

6/94 **Offentlige informasjonstjenester: Rettslige aspekter**
Jon Bing.....*NOK148.-*

7/94 **Sattelittfjernsyn og norsk rett. MERETE (3) IV**
Nils Eivind Risvand .....*NOK 138.-*

8/94 **Videogram på forespørsel. MERETE (14) IV**
Beate Jacobsen (red).....*NOK 158.-*

9/94 **«Reverse engineering» av datamaskinprogrammer. TERESA (92) IV**
Bjørn Bjerke.....*NOK 198.-*

10/94 **Skattemessig behandling av utgifter til anskaffelse av datamaskin-programmer. TERESA (75)**
Gjert Melsom.....*NOK 198.-*

1993

1/93 **Artificial Intelligence and Law. Legal Philosophy and Legal Theory**
Giovanni Sartor .....*NOK 148.-*

2/93 **Erstatningsansvar for informationstjenester, særlig ved databaseydelser**
Connie Smidt .....*NOK 138.-*

3/93 **Personvern i digitale telenett**
Ingvild Hanssen-Bauer.....*NOK 178.-*

4/93 **Consumers Purchases through Telecommunications in Europe. - Application of private international law to cross-border contractual disputes**
Joachim Benno.....*NOK 198.-*

5/93 **Four essays on: Computers and Information Technology Law**
Morten S. Hagedal.....*NOK 218.-*

6/93 **Sendetidsfordeling i nærradio MERETE (3) III**
Marianne Rytter Evensen .....*NOK 148.-*

7/93 **Essays on Law and Artificial Intelligence**
Richard Susskind .....*NOK 158.-*

1992

1/92 **Avskriving av mikrodatamaskiner med tilbehør – en nordisk studie TERESA (87)**
Beate Hesseltvedt.....*NOK 138.-*

2/92 **Kringkastingsbegrepet TERESA (78)**
Nils Kr. Einstabland.....*NOK 208.-*

3/92 **Rettskilderegistre i Helsedirektoratet NORIS (94) I & II**
Maria Strøm.....*NOK 228.-*

4/92 **Softwarepatent – Imaterialrettens enfant terrible. En redegjørelse for patenteringen af softwarerelaterede opfindelser i amerikansk og europæisk ret**
Ditlev Schwanenfügel.....*NOK 158.-*

5/92 **Abonnementskontrakter fro kabelfjernsyn TERESA (78II)**
Lars Borchgrevink Grindal .....*NOK 248.-*

6/92 **Implementing EDI - a proposal for regulatory form**
Rolf Riisnæs.....*NOK 118.-*

7/92 **Deponering av kildekode«escrow»-klausuler TERESA (79)**
Morten S. Hagedal .....*NOK 128.-*

8/92 **EDB i juridisk undervisning – med en reiserapport fra England og USA**
Ola-Kristian Hoff.....*NOK 228.-*

9/92 **Universiteters ansvar for bruk av datanett TERESA (94)**
Jon Bing & Dag Elgesem .....*NOK 198.-*

10/92 **Rettslige sider ved teletorg**
Andreas Galtung.....*NOK 148.-*

BESTILLING

Jeg bestiller herved følgende CompLex-utgivelser:

Nummer / årgang: _____
Tittel: _____

Nummer / årgang: _____
Tittel: _____

Nummer / årgang: _____
Tittel: _____

Nummer / årgang: _____
Tittel: _____

Nummer / årgang: _____
Tittel: _____

Navn: _____
Adresse: _____
Postadresse: _____
Telefon: _____

Bestillingsskjemaet sendes pr.post eller telefaks til:

Avd. juridisk litteratur Aulabygningen
Karl Johansgt. 47, 0162 Oslo
Telefon: 22 42 54 50
Telefaks: 22 41 17 08

CompLex kan også bestilles via nettbokhandelen www.gnist.no