River Information Services
Electronic Reporting International

ERI Guide Part I

General introduction and functional description of electronic reporting

Version 2.0
31 August 2006

Table of content

1. Preface

Over the past years all members of the expert group Electronic Reporting International have, in cooperation with the users of inland waterways, worked intensively to prepare, test and evaluate the possibilities of Electronic Reporting. This guide and documents are the result of their contributions. As Chairman of the Expert group I would like to thank all persons involved for their time, work, knowledge and efforts, without their commitment it would have been impossible to complete our mission.

My special thanks go to the following members of the sub-working group of the ERI expert group who made a tremendous effort during the last months in writing down and discussing the included messages, standards and procedures.
Mr. A. A. de Lijster, functional advisor Rijkswaterstaat the Netherlands
Mr. P.F. Oudenes, technical advisor Rijkswaterstaat the Netherlands
Mr. P. Nefkens, representative of the Dutch Inland Shipping Organisations
Mr. M. Sattler, Via Donau Austria
Mr. N. Braunroth, WSD Germany
Mr. H. Wepper, FVT Germany
Mr. C. van de Weerd, Port of Rotterdam
Mrs. C. de Leleu VNF France
Mr. R Bollengier VNF France
Mr. O Dissaux VNF France

Acknowledgements
This difficult task would not have been possible without the enthusiastic support of Mr. C. Krajewski who succeeded the past years is setting up the Ship Reporting Standard. This standard was the basis for all further actions on standardisation of the included messages, procedures and reference tables and who I would like to thank especially for his vision and guidance.

With this I also want to honour Mr. Robert Scherpbier. Without his optimistic approach, knowledge on the field of message standardisation and implementation and his strategic vision and overview we would not have been where we are at present.

J. van Splunder.

2. Introduction

The ERI guide to electronic reporting consists of four parts with one or more annexes, The first two parts are dealing with the introduction and functional aspects of electronic reporting. These parts are meant to serve as a guidance, introduction and explanation of the used standards and related issues in electronic reporting.

- Part I, is dealing with the introduction and the functional description of electronic reporting.
- Part II, is dealing with protection of data and code of conduct

Parts III and IV represents the technical specifications of the standards

- Part III, is dealing with Implementation manuals
- Part IV is dealing with codes and references

The Guide and in particular parts III and IV which contain the technical specifications of the used standards must be considered as a stable document, to ensure harmonised and standardised RIS implementation of electronic reporting. The reason for separate annexes for the message implementation manuals lies in the fact that to facilitate efficient updating and maintenance, the annexes have to be maintained separately and under its own regime of change requests and update numbers.
This regime will be defined separately by the ERI group.
The guide is meant to provide a set of guidelines and responsibilities for users and decision makers of Electronic Reporting International (ERI) in the implementation and usage of software for the exchange of electronic information.
The term EDI (Electronic Data Interchange) used in this guide is meant to cover all forms of electronic transfer of structured data in accordance with the relevant international standards such as UN/EDIFACT, XML and any other agreed syntactical solutions.
The usage of electronic data is increasingly replacing the need for paper documents and manual procedures but to get maximum benefits from this development it is of the utmost importance that agreements are in place on the use of electronic messages, the data to be exchanged, the used codes and references and the procedures related to privacy, integrity and security.
To ensure a clear division of responsibilities regarding the exchanged data it should be realised that electronic reporting and other ways of data interchange are always managed and executed by the owner of the information or by the party appointed by the owner of the data. However an appointed party will always act on behalf of the owner and will only provide information and or electronic data to the authorities, organisations and / or companies which are agreed upon by the rightful owner of the information.

As a final goal, electronic reporting and electronic messaging in general should lead to a paperless environment in inland shipping with the assurance that all necessary information will be available at the right time, in the right place with the appropriate parties, to ensure a fast despatch and simple transparent procedures with appropriate controls and simplified inland water transport processes.

In accordance with the code of conduct and privacy rules, the following items are to be seen as references for the exchange and collection of data.

- Confidentiality:

The majority of the messages that will be transferred will contain information about the location of a ship, data about the ship, the people on board and/or the cargo it is transporting. Some of this information can be valuable to competitors, criminals and even terrorists. Thus, the information has to be kept confidential, except for the rightful receiving party.
This means that the information, where necessary, need to be encrypted in such a way that it can only be decrypted by the receiving party; additionally, the sending party must have means to authenticate the recipient in order to avoid communicating the confidential information to an impostor.

- Integrity

In addition to keeping the transferred messages secret, they need also to be protected from unauthorized modification while in transit from one system to another. A means must be provided to enable the receiving party to detect whether the message has been altered or corrupted.

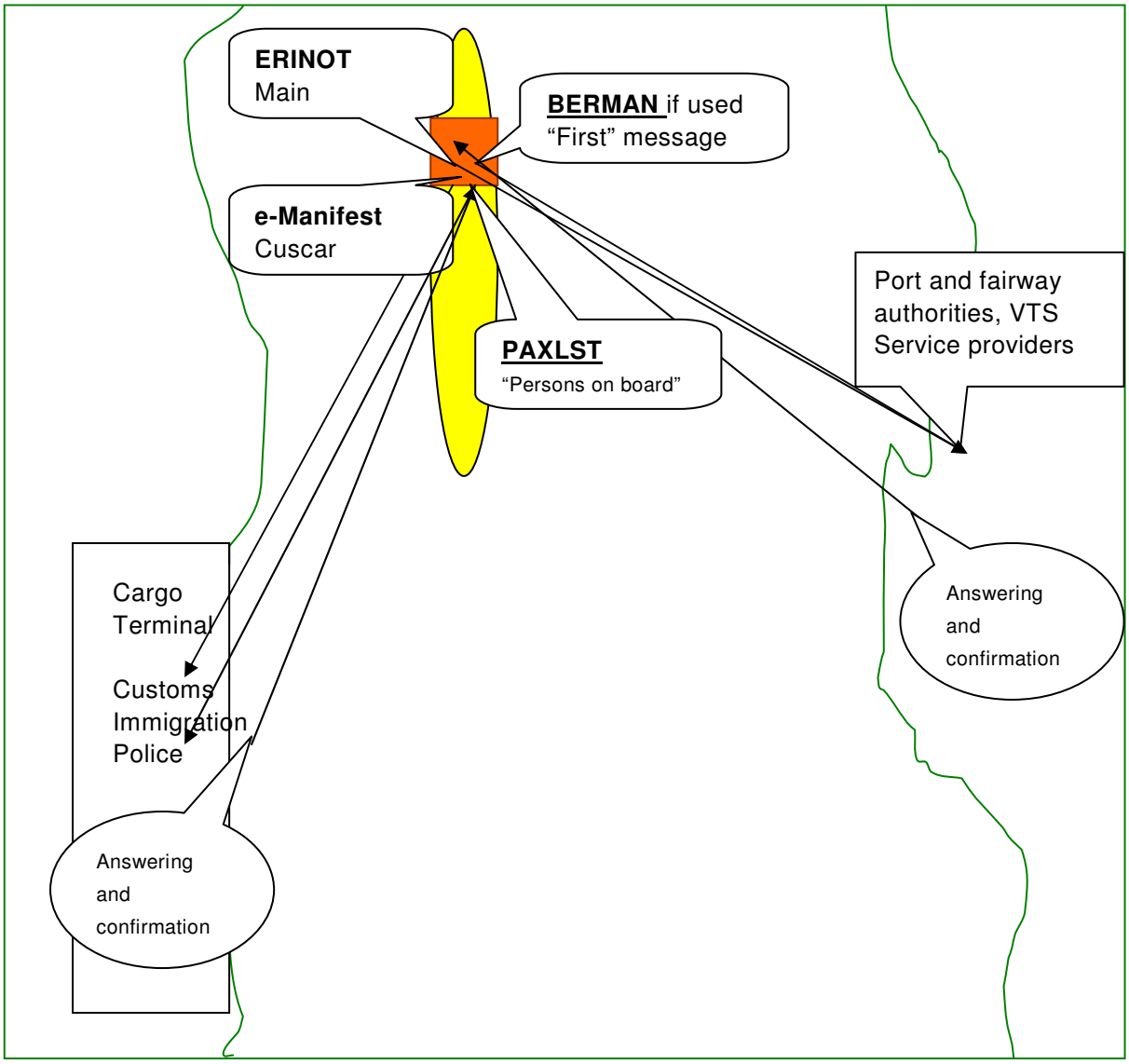
- Sender is always responsible

Because the sender of the information is always responsible for the information being sent, it must be ensured that during the handling of the messages the integrity of the data in the messages needs to be guaranteed in all cases.
In case of modification of the message (for instance during an EDI translation), this might pose a challenge to ensure that the owner of the information can maintain his responsibility for the correctness of the data.
Where untrue particulars are furnished in an electronic report and it can be shown that all reasonable steps had been taken to provide accurate and correct information this factor shall be taken into account in considering any further action. Where such misinformation occurs as a result of force majeure or other circumstances beyond the control of the sender concerned and there is no question of negligence or other intent, no further action shall be taken provided that the facts are duly established to the satisfaction of the authorities concerned.

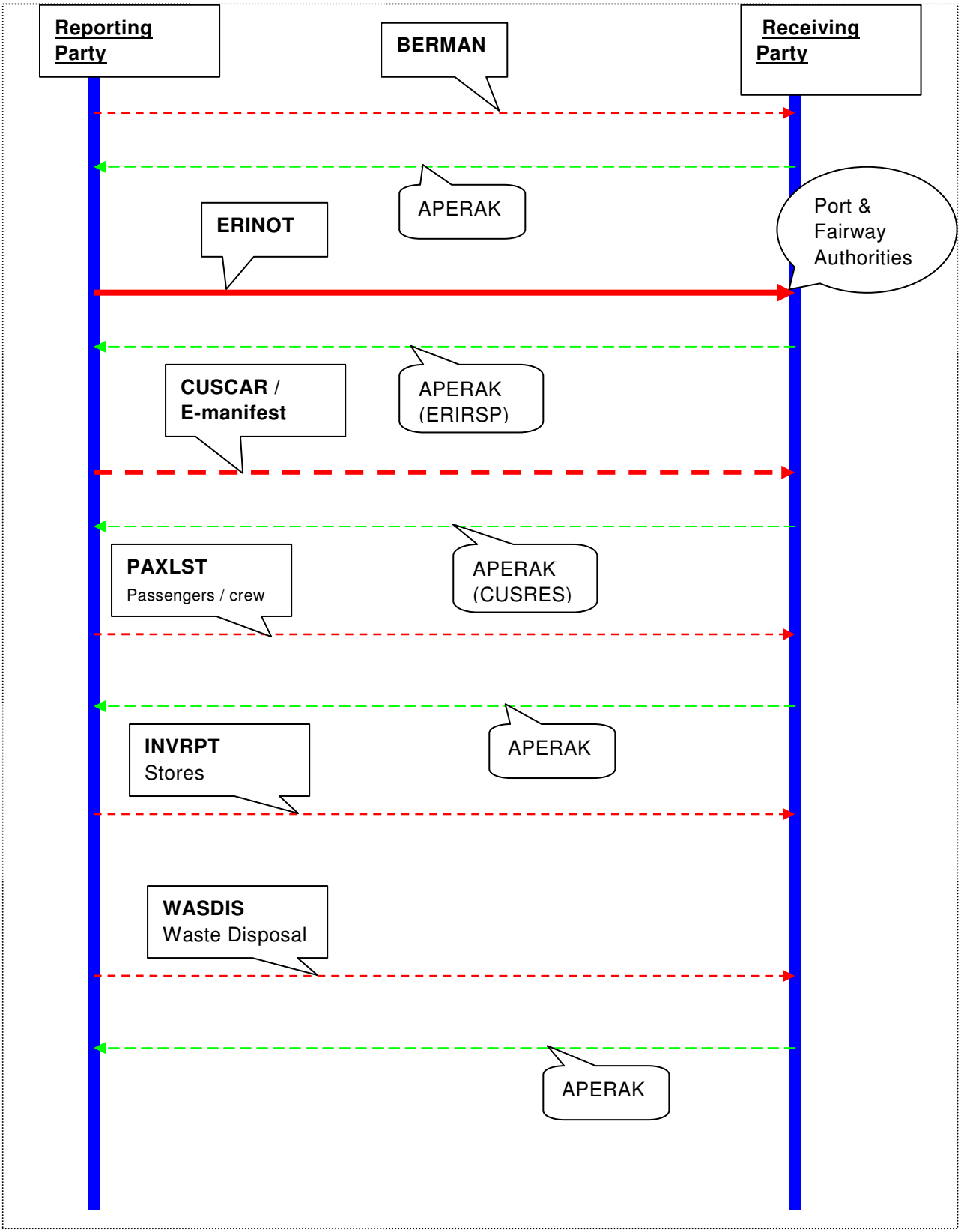
Technical specifications dealing with the details of the security aspects of EDI messages, such as for instance the need for common encryption methods, will be dealt with separately through the ERI group of experts.

3. Messages and their functionality

The following messages have been foreseen to cover the respective described functionalities



Possible Sequence of messages



3.1 ERI notification message (The reporting message)

The ERI notification message (ERINOT) must be used for the reporting of dangerous and non dangerous cargo carried by inland waterway vessels. The ERINOT message is a specific use of the UN/EDIFACT 'International Forwarding and Transport Dangerous Goods Notification (IFTDGN)' message such as has been developed within the PROTECT organisation. This standard message has been accepted by the IMO/FAL for the reporting of dangerous goods to authorities. The applied version has been included in the IMO (International Maritime Organisation) Compendium on Electronic Business. It is the message from the party responsible to report “dangerous” goods to the authority performing the control and checks on conformance with the legal requirements. The message is conveying information on the “dangerous” goods being loaded, discharged and/ or in transit relating to a means of transport such as ships used for inland waterway transport

Where reporting is mandatory and if technically feasible, an ERI notification message is to be composed and sent to the competent authority for each inland waterway transport. However vessels are invited to report electronically to the competent authorities whenever possible.

The notification message based on this standard message can be depicted as follows:

“ERI (Electronic Reporting International) Notification Message” with the following types:

- transport notification from vessel to authority from ship to shore;
- transport notification from carrier to authority from shore to shore;
- passage notification from authority to authority.

3.2 Berman Message Version 2

The Berth Management message combines the pre-arrival notification respectively general declaration combined into one single notification which is based on the EDIFACT message BERMAN from the UN/EDIFACT D04B directory the implementation manual and guidelines are based on the guidelines as given by the Protect group of ports.
The message is sent by the vessel before arriving at or departing from a berth or a port giving particulars about the time of arrival, the services required and any particulars necessary to ensure prompt handling of procedures and facilitating controls.
The message incorporates the (legal) requirements regarding the notification of a ship to a port. It supports one request for the ship - be it for entering the port, berthing on arrival of the ship, leaving the berth on departure of the ship or shifting of berths for the ship within the port or for only transiting through the port area. The arrival and transit notification contains all details regarding the movement of the ship from outside the port area to the first berth in the port area or in case of transit traffic to the point where the vessel is leaving. Required additional services to be arranged for arrival at a berth may be specified.
The ETA at the entry point and where required leaving point and previous place of call of the ship are required information elements.

3.3 e-Manifest / Customs Cargo Report

Manifest message
A message from the party providing the transport/ forwarding services to the party that issued the instructions for those services and the involved governmental authorities charged with compliance controls, stating the actual details, terms and conditions of the service and of the consignment involved. In addition it can be used for the exchange of information with other authorised parties in the transport chain.

3.4 Passenger and crew-lists

Where national privacy legislation permits, and with the agreement of all parties involved, this Passenger / Crew List message (PAXLST) permits the transfer of passenger/crew data. The message may be exchanged between Captain/Skipper or Carrier (such as inland waterway operators) and Customs, Immigration, Police, ISPS Terminals or any designated authorities.
The message can also be used to transfer passenger / crew data from a Customs, Immigration or other designated authority in the country of departure to the appropriate authorities in the country of arrival of the means of transport.
The transfer of data may occur prior to arrival of the vessel at the place where controls may take place. This is to permit the designated authority at the place of

destination to screen this data and take timely decisions related to the clearance of passengers and crew e.g. pre-arrival clearance.
The availability of passenger and crew information is especially important whenever search and rescue operations need to be carried out. So for calamity abatement purposes the availability of passenger and crew lists is crucial.

3.5 APERAK General Response and receipt message

This message is used to provide where required for a number of answering and response functions on messages which have been sent such as:

3.5.1. The ERI RESPONSE MESSAGE ERIRSP

The response message is generated by for instance a RIS centre. This ERIRSP message is derived from this UN/EDIFACT APERAK message. The response messages on the respective functions (new, modification or cancellation) of the ERI notification message ERINOT all have the same structure. The response on a modification or a cancellation contains information whether or not the modification or cancellation has been processed by the receiving system.

3.6 Other contemplated messages:

Where required message user guidelines of the following messages might be added to the annex of ERI Guide Part III in a later stage:

- ships stores declaration (INVRPT);
- voyage plan;
- lock plan;
- waste disposal (WASDIS);
- port and fairway dues collection.

4. System overview of electronic reporting

This chapter gives an overview of the four basics components, which are necessary for electronic reporting as it is provided within the use of the ERI Cross Border software.

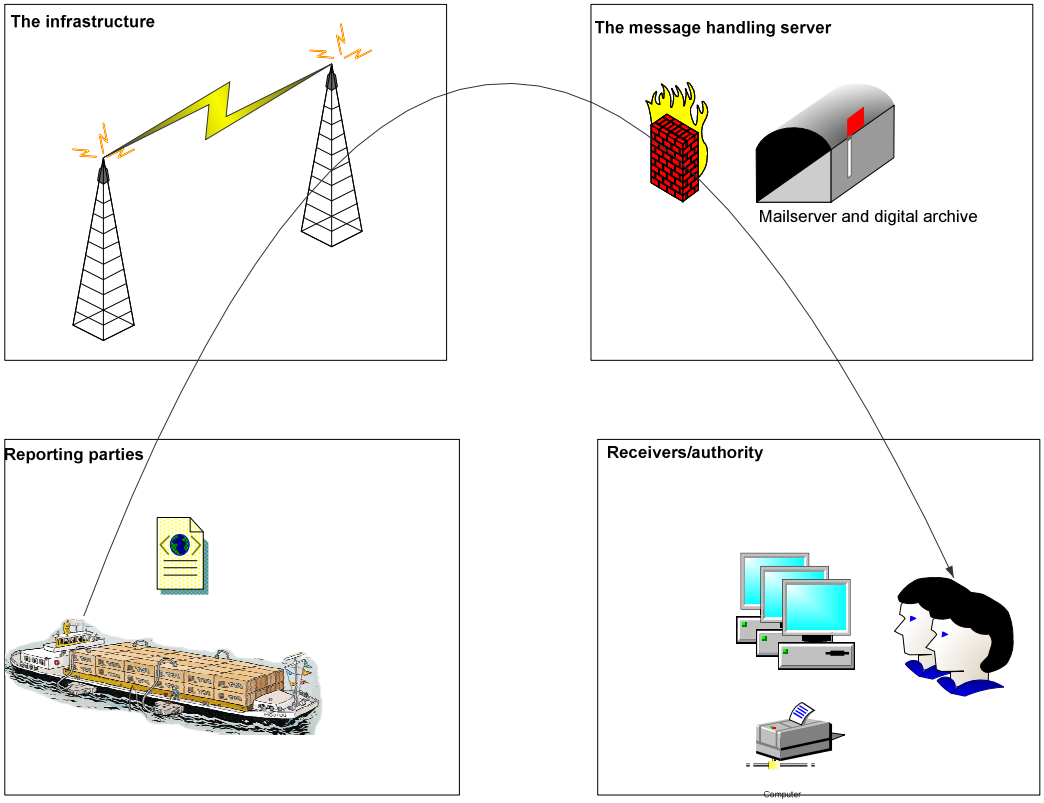


Figure 1: System overview of the electronic reporting (based on ERI Cross Border Software architecture)

Either the captain/skipper, fleet operator or the shipper of the cargo are, according to the respective regulations in most countries, obliged to report to the competent authority in the country where the vessel starts its voyage upon the departure of a vessel. When crossing borders, the vessel has to report again to the competent authority of the entered territory. In the past the reporting was normally done via VHF communication (voice) or by fax. Electronic Reporting offers possibilities for vessels to report the voyage, cargo, and persons on board in a more convenient way additional to voice or paper form reporting.

Using a reporting application, a vessel or a party reporting on behalf of the vessel can create and submit the report electronically via available infrastructure to the message processing system (this message processing system can be provided by the RIS operators in each country). From there, the reports are either automatically forwarded to the recipients (e.g. competent authorities) or can be directly retrieved and displayed by the recipients (e.g. competent authorities) who have access to the message archive.

4.1 Reporting parties

Reporting parties are the actors in the transport chain responsible for submitting information, either sent by or on behalf of the vessel, to the competent authorities and governmental agencies.

The following parties are considered to report the transport related information, such as voyage, cargo and personal related information:

- Ship master / captain / skipper
- Fleet / Vessel operators
- Ship agent / Freight forwarder / Shipper
- Authorities on behalf of the vessel (forwarding voyage related data of the vessel)

A reporting application enables the reporting party to enter all relevant information within an appropriate software tool, which is then automatically creating the electronic reports out of the entered information based on the technical specification for electronic ship reporting (ERI standard messages).

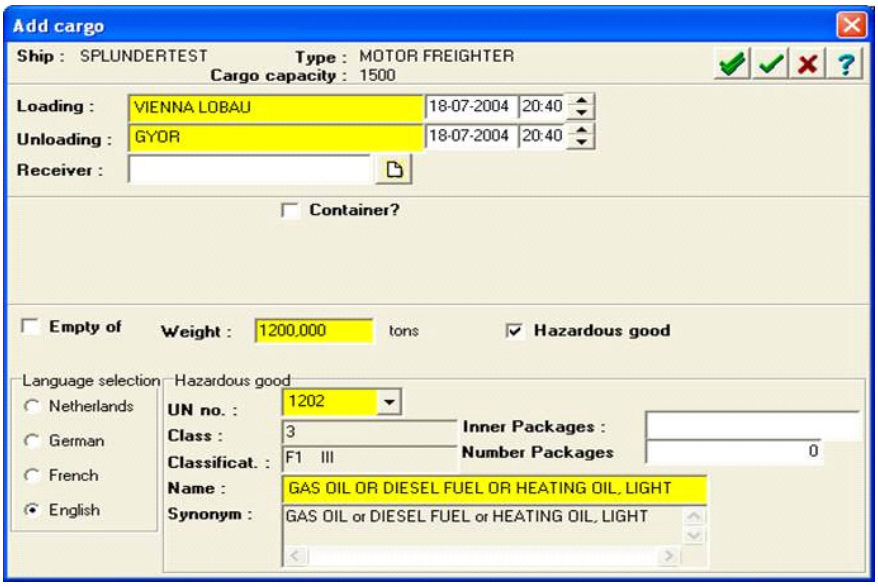


Figure 2: Screenshot of ERI CB Software

Furthermore the created electronic reports (standardised messages) can be sent easily to the relevant receivers (e.g. competent authorities) via appropriate infrastructure.

4.2 Infrastructure

A communication infrastructure needs to be available to exchange messages (submit electronic reports and acknowledgements) between the reporting party and the recipients (for instance the competent authorities). Besides a general infrastructure (e.g. telephone network, broadband connection, GSM, GPRS, UMTS) users do need suitable equipment to connect to this general infrastructure (PC or Laptop with access to internet or any other appropriate communication medium).

4.3 Message Handling System

The message handling system is based on two separate systems.
These systems are:

- a secure message server;
- a digital archive.

Secure message server (mandatory)
The electronic reporting software will deliver the electronic reports to a secure message server. This secure message server will deliver the electronic reports to the competent authorities, taking into account all privacy and security aspects.

Digital Archive (Optional)
This archive is necessary to administer, maintain and safely store the received electronic reports, whilst taking into account all privacy aspects. Various user accounts have to be necessarily established in order to enable authorised receivers to retrieve individual information (stored electronic reports) from the message archive under pre-defined access-rights.

For the implementation of the message handling system a number of possibilities can been considered.

- Centralised solution: One single message handling system including one central message archive is implemented and can be used by all parties (international level) involved in the electronic reporting process. This is maybe the technical most convenient solution but raises questions about financing the implementation, maintenance and operating costs. Furthermore privacy related issues are getting a delicate problem.
- Decentralised solution: Each country implements its own message handling system and message archive including an appropriate interface to exchange relevant data with message processing systems and message archives in other countries. This is technically a bit more complicated but easier to implement on organisational level. Furthermore the responsibility for proper data processing is not assigned to only one party.
- Combined solution: As a kind of combination, a third possibility could be that two or more countries implement one centralised message processing system and message archive together with countries connected to other centralised or decentralised message handling systems.

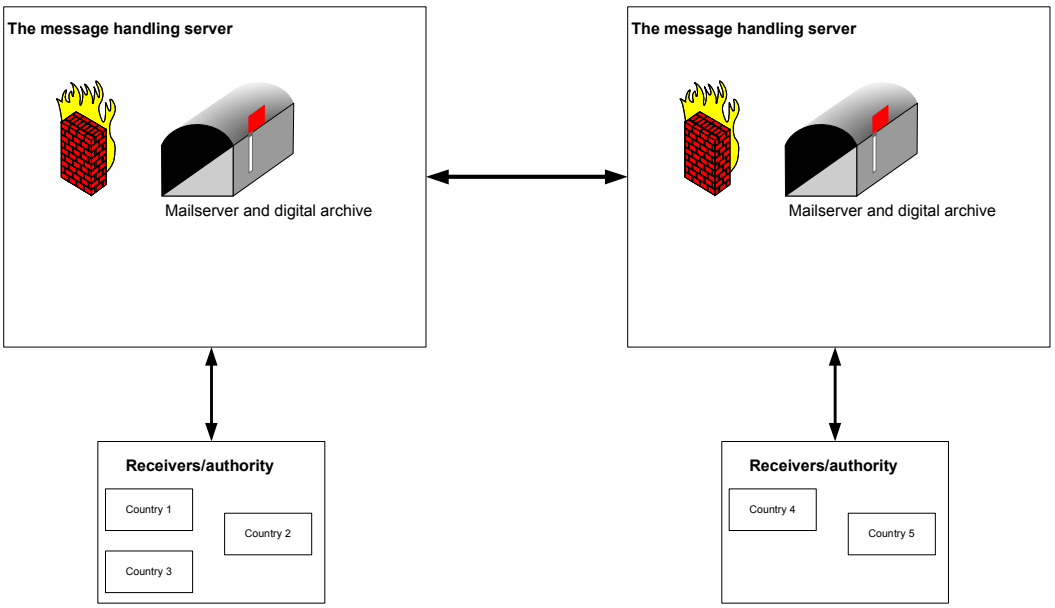


Figure 3: Combined solution

4.4 Receiving parties

Receiving parties are principally the competent authorities, and where applicable those commercial parties who are entitled, and nominated as such, to receive all or part of the information submitted by the reporting parties.
The competent authorities dealing with electronic reporting are:

- VTS operator
- Traffic / Fairway authorities
- Lock / Bridge operators
- Harbour master / Port authority
- Police
- Customs authorities
- Immigration
- Inspection authorities
- Veterinary / Phytosanitary inspection authorities
- Authorities responsible for charging of waterway dues
- Calamity centre
- Statistics offices

The operational, commercial organisations which might also benefit from the electronic exchange of information are:

- Terminal operators
- Vessel operators (and others as specified by the ship master)
- Consignees
- Shippers
- Skippers / Captains

(This document does presently not deal with the information exchange with these commercial parties)

There are several possibilities for the receiving party to get relevant information out of the electronic reporting system.

- With the use of an appropriate message receiving application, the reports which are addressed to a user of this application (user access rights have to be defined during installation) are directly forwarded to the receiver by the message handling system.
- Within a separate system, the distribution mechanism and the retrieving as well as displaying of the relevant information and reports can be implemented individually.
- Each party with appropriate pre-defined access rights can retrieve relevant reports directly from the message archive.
- The reporting party itself can also enter email addresses when creating the electronic reports to which the relevant reports will be sent via email in appropriate format directly via the infrastructure and message handling system.

5. Security in electronic data interchange

5.1 Objective

The objective of Security in EDI is to define and implement means and measures to enable secure communication between government authorities and inland water transport operators.
More comprehensive, it aims to ensure that appropriate controls to maintain the integrity of transactions and their related authorization throughout the communication process are defined and in place.

5.2 Sender is always responsible

The sender of the information is always responsible for the information being sent. This means that the integrity of the information has to be guaranteed in all cases. In case of modification of the message (for instance EDI translation), this can pose a challenge for third party services but will need to be dealt with, to ensure that the information remains exactly the same in whatever way the information is sent.

5.3 Ensuring secure EDI communication

1. Distinguish between different kinds of transactions that have to be secured;
2. Investigate how these transactions currently take place;
3. Realize a common understanding within the context of ERI with respect to the minimal required security levels for different kinds of transactions;
4. Define means and measures to implement those minimal requirements in a way that this implementation can be expanded to the desired security level;
5. Implement these means and measures
6. Expand the implementation guidelines to reach the desired security level.

As indicated in the introduction of the ERI Guide, technical specifications dealing with the details of the security aspects of EDI messages such as for instance the need for common encryption methods will be dealt with separately through the ERI group of experts and will be part of a separate annex.

5.4 Security law and regulation

National laws and regulations regarding design and security are often an application or direct implementation of the laws, regulations and guidelines of the European Communities. Some aspects of security are at present not yet covered in European context and in those cases some countries have implemented their own choice of regulations and techniques.
As a result the laws and regulations that apply to all participating countries must be considered the sum of all the national laws and regulations in effect in those countries.
As there are different levels of security regulations in the different countries, the data exchange between two countries must be based on similar regulations in those two countries. A MoU(Memorandum of Understanding) between these countries might ensure a common legal base.
This situation will change as soon as the European legislation harmonises the various national rules and regulations.
The desired ultimate solution should in future also apply to non-EU countries.
Current certificate authorities are defined at a national level. There is presently no overall international organisation that covers all participants throughout Europe. The aspect of common legislation needs to be discussed and solutions provided through the committee dealing with River Information Services.

The following kinds of exchanges do have a need to be secured:
- electronic clearance;
- crew and passenger lists;
- delivery of cargo and voyage information;
- toll levying, invoicing, and related notices;
- sailing licenses and or permits.

For each category of transaction the desired security level should be determined.

5.5 Security demands

In order to ensure security for the transactions mentioned above, the following security demands can be discerned.

- Confidentiality
  The majority of the messages that will be transferred will contain information about the voyage of a ship and/or the cargo it is transporting. This can be valuable information to criminals and even terrorists. Thus, the information will need to be kept secret, except for the receiving party.
  A solution is that the information is encrypted in such a way that it can only be decrypted by the receiving party; additionally, the sending party must than have the means to authenticate the recipient in order to avoid communicating the confidential information to an impostor.
- Integrity
  In addition to keeping the transferred messages secret, they should also be protected from unauthorized modification while in transit from one system to

another. A means has to be provided to enable the receiving party to detect whether the message has been altered or corrupted.

- Non-repudiation
  Message integrity is not only necessary in order to ensure the correct workings of the system but is also a requirement for non-repudiation. Non-repudiation provides proof for the integrity and origin of data, so the sender can be held responsible for the data being sent. It is achieved through cryptographic methods and it prevents an individual or entity from denying having performed a particular action related to data (such as mechanisms for non-rejection or authority (origin); for proof of obligation, intent, or commitment, or for proof of ownership).
- Verifiability/ audit ability
  Records of all transactions must be kept in such a way that this can support an audit to determine whether all transactions and their processing have occurred as claimed. This will need to include archival of the messages being sent or received or rejected
- Voyage related Information sent only once
  All information concerning a vessel, its voyage, or its cargo should be entered and sent only once. This implies that any server to be used should be able to duplicate information and make it available to those parties that have a legal right to this information.

5.6 Security Infrastructure

Since the connections might take place over public networks like the Internet, the security level of these connections needs to be at an adequate level. This can be done by using SSL/TLS encryption or by means of a VPN.

6. Exchange between Authorities

The availability of information is based on predefined roles for a single governmental organisation such as Waterway Authorities. This does imply that the information is not automatically available for all other governmental organisations within the country or to all authorities in the other countries affected by the transport. The interchange agreement and code of conduct are quite clear on all aspects of the protection of privacy and the legal requirements for certain data of the various authorities. The usage of Single Window techniques does need to ensure that not more than the legally required information will reach the competent authority or the appropriate governmental organisation.

For Customs purposes the use of Electronic exchange of information has taken a solid hold in quite a number of countries. The Kyoto Convention has created possibilities to transport goods without paper documents for customs control. It goes without saying that the large-scale transfer of cargo information and goods declaration data from traders and transport operators to Customs is ideally suited to the application of EDI techniques. Whilst originally the extensive use of EDI by customs administrations related principally to the clearance of goods for import and export, the introduction by DG TAXUD of NCTS has now also created good opportunities for the control of the goods in Transit.

It is envisaged that the application of electronic exchange of information will continue to show a strong growth pattern over the coming decade. However as the role of Customs expands, taking into account also the need to deal in some instances not only with information on goods but also with security aspects, and as new ways of performing old tasks emerge, there will be an increasing need to exploit other possibilities afforded by the use of electronic information in its broadest sense.

To accommodate the needs of national governmental administrations and other official parties involved the administrations will be expected to enhance and/or re-engineer their internal processes in line with the driving factors such as:

- expectations of inland transport (improved service levels and information access);
- national economic and security interests (faster goods and vessel clearance, enhanced revenue and border protection);
- streamlining of the operations of the governmental organisation (e.g. automation of routine processes, focussed enforcement and compliance checking, improved working environment and efficiency.

This leads to the following legal and policy implications for the authorities exchanging information:

- appropriate practices, policies and technical solutions in line with this guide to ensure privacy, confidentiality, integrity and accuracy;
- to consider ways of encryption, public key infrastructure and certification authority, digital signatures;
- security of messages;

- authentication;
- non-repudiation;
- fraud and misuse prevention;
- intellectual property protection;
- human resource implications.

See also in this respect the Code of Conduct contained in Part II of this Guide

The availability of information in electronic form prior to the arrival of a vessel would allow the competent authorities to run their risk assessment and controls on the vessel and its cargo creating possibilities to inform the captain / skipper electronically about any decision prior to arrival.

The sharing of information between authorities will where possible lead to the acceptance of previous controls by another state agency which may in its turn lead to less double or triple work because once a control is done and there are no changes, the results of this control should be recognised by all authorities along the route of the ship.
For receiving relevant information out of existing electronic reporting systems, the authorities have to be integrated as receiving parties into the electronic reporting process. Therefore close cooperation between the authorities and the operator of River Information Services responsible for the operation of the electronic reporting system is of utmost importance. Here the use of Single Window Concepts will be an opportunity.
Interchange agreements between the authorities, national and international, must be seen in this context as a very important clarification and division of the responsibilities of for instance the RIS operators and the owners of the information. *See also Part II of the ERI Guide and the annex for an overview of the data.*

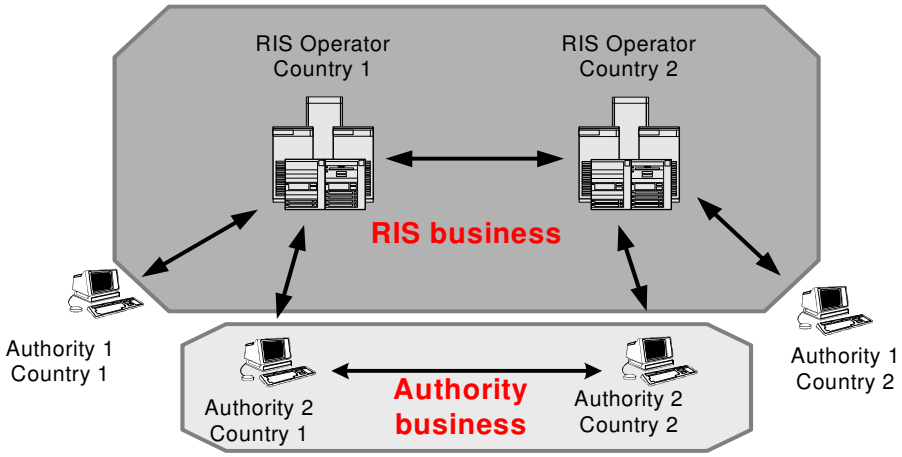


Figure 4: Division of responsibilities within electronic data exchange between for instance Germany and the Netherlands.

From this overview it should be clear that information provided for operational purposes can not always be available for the purposes of authorities not dealing with the river services. This needs to be cleared in the Interchange agreement and in accordance with the information given in Part II of the ERI Guide.

7. Interchange Agreements

An interchange agreement sets out the rules the parties will adopt for using Electronic Data Interchange. The agreement also defines the individual roles and legal responsibilities, in accordance with the respective legislation, of the parties for transmitting, receiving and storing electronic messages.

The agreement seeks to provide EDI messages with a legal binding effect across sometimes different national legal systems. This goal is pursued by addressing all of the basic legal issues needing to be covered before EDI messages can be used to fully replace paper documents.

Agreement is required on at least the following issues:

1 selection of the type of EDI messages, message standards and methods of communication;
2 responsibilities for ensuring that the equipment, software and services are operated and maintained effectively;
3 procedures for making any system changes which may impair the ability of the parties to communicate;
4 security procedures and services;
5 the points at which EDI messages have legal effect
6 the roles and contracts of any third party service providers
7 procedures for dealing with technical errors
8 the needs for confidentiality
9 liabilities in the event of any delay or failure to meet agreed EDI communication requirements;
10 the laws governing the interchange of EDI messages and the arrangements of the parties;
11 methods for resolving any possible disputes.

In the following section a framework for an interchange agreement will be included as a model to cover the respective legal requirements for the international use of electronic data interchange.
The model contains a clear and unambiguous statement that it is the intention of the parties to be bound by the Agreement; this emphasizes that the parties (organisations) desire to operate with, and not outside, a legal framework with respect to their use of Electronic Data Interchange.
An interchange agreement is intended to provide a strong legal basis for ensuring that EDI communications will have a legally binding effect and subject to national laws and regulations will enable the substitution of documental evidence and the replacement of paper documents.

7.1 Model of an Interchange Agreement

SECTION 1 SCOPE AND STRUCTURE

1.1 Scope:
This agreement governs any electronic transfer of Messages between the parties as defined in the ERI Guide. Except as expressly provided, this Agreement does not govern any other relationships, contractual or not, in the context of which Messages are communicated. A message means data structured in accordance with the internationally agreed standards as contained in the ERI Guide and its attachments.

1.2 Technical Annex:
The message implementation guidelines respectively manuals set forth the user specifications agreed upon by the parties for the technical data requirements. In the event of a conflict between the terms of this agreement and the implementation guidelines – manuals, the terms of this agreement shall prevail.

SECTION 2: COMMUNICATIONS AND OPERATIONS

2.1 Standards
The agreed standards are those standards established for Electronic Data Interchange (together with the related Recommendations) as agreed by the standardisation organisations such as UNECE and approved by the ERI Working Group of the RIS Committee. The parties shall use those versions of the standards identified in the implementation guidelines in the annex.

2.2 System Operations
Each party shall test and maintain their respective equipment, software, and services necessary to effectively and reliably transmit and receive Messages.

2.3 System Changes
No party shall make any changes in systems operations which impair the mutual capabilities of the parties to communicate as contemplated by this Agreement without providing prior notice of the intended change.

2.4 Communications
The methods of communication, including the requirements for telecommunication or the requirements towards the third party providers shall be specified by the ERI Working Group and will be part of this guide.

2.5 Security Procedures and Services
Each party shall implement and maintain security procedures and services specified in the ERI Guide and attached implementation manuals, to protect Messages and their records against untoward events or misuse including improper access, alteration or loss.

2.6 Record Storage
The parties shall store and retain records and the messages communicated under this Agreement as may be specified in the ERI guide.

SECTION 3: MESSAGE PROCESSING

3.1 Receipt
Any message transmitted in compliance with this Agreement shall be deemed received when accessible to the receiving party in the manner designated in the implementation manual. Until so received, no transmitted Message shall have any legal effect unless applicable law mandates legal effect to such Message upon transmission, whether or not received.

3.2. Acknowledgement

3.2.1 Unless otherwise designated in the Implementation Guidelines, the receipt of a Message need not be acknowledged by the receiving party. A requirement for acknowledgement in the Implementation Guidelines shall include the methods and types of acknowledgement (including any messages and procedures) and the time periods, if any, in which acknowledgement must be received.

3.2.2. Where required an acknowledgement will be prima facie evidence that the related Message was received. A party receiving a Message requiring acknowledgement shall not act upon that Message until the acknowledgement is sent. If a receiving party is not able to send the acknowledgement, it shall not act upon the Message without further instructions from the sender of the Message. The failure of a receiving party to acknowledge a Message will not deprive the Message of its legal effect, except when the originating party is not identifiable from the Message.

3.2.3 In the event that the originating party has not received, for a properly transmitted Message, a required acknowledgement and no further instructions have been provided, the originating party may declare the Message null and void by so notifying the receiving party.

3.2.4 Technical errors. A receiving party must give notice to the originating party of circumstances, including technical errors in a received transmission, which prevent the further processing of a Message.

SECTION 4: VALIDITY AND ENFORCEABILITY

4.1 Validity
The parties agree that valid and enforceable obligations may be created by the communication of Messages in compliance with this Agreement. The parties expressly waive any rights to object to the validity of a transaction solely on the ground that communication between the parties occurred through the use of Electronic Data Interchange.

4.2 Evidence

Without regard to the absence of any writings and written signatures to the extend permitted by law, the records of Messages maintained by the parties shall be admissible and may be used as evidence of the information contained therein.

SECTION 5: DATA CONTENT REQUIREMENTS

5.1 Confidential Status

No information contained in any Message communicated under this agreement shall be considered confidential unless by operation of law or by designation in the ERI Guide.

5.2 Legal Compliance

Each party shall ensure that the content of any Message is transmitted, received or stored in compliance with all legal requirements to such party
In the event that the receipt or the storage of any element of a Message would constitute a contravention of the applicable law, e.g. the governing privacy rules, the receiver shall without undue delay give notice of such non-compliance.

SECTION 6: LIABILITY

6.1 Force Majeure

No party shall be liable for any delay or other failure in performing its obligations under this Agreement where such delay or failure is caused by any event beyond the party's control

a. which could not be reasonably expected to have been taken into account at the time this agreement was concluded
b. the consequences of which could not be avoided or overcome.

6.2 Excluded damages

No party shall be liable for any special, consequential, indirect or exemplary damages arising from any breach of this Agreement.

SECTION 7: GENERAL PROVISIONS

7.1 Governing Law

This agreement shall be governed by the regulations of the European Communities, the applicable National legislation and the rules of the international inland waterway transport committees (e.g. CCNR, Danube Commission)

7.2 Severability

Should any provision of this Agreement be invalid or unenforceable for any reason, all other provisions of the Agreement shall remain in force and effect.

7.3 Termination

Any party may terminate this Agreement upon not less than [30] days prior written notice of the termination. No termination shall affect any communications occurring prior to the termination, or the performance of any related transactions. The sections concerning protection of data and confidentiality shall expressly survive any termination and remain binding upon the parties.

7.4 Entire Agreement

This Agreement, including the ERI Guide and the attached implementation manual - guidelines, constitutes the complete agreement of the parties on the subject matters of this Agreement and becomes effective when agreed by all involved parties. The Implementation Guidelines may be amended by the parties involved in the exchange of information and by the persons authorised by the ERI Working group on behalf of the RIS Committee to deal with amendments in accordance with the Change Request procedures. Each party shall be provided with advance notification of every amendment agreed upon by the ERI Working Group as indicated in the records of the working group with sufficient time to ensure implementation. Such changes will be recorded in the Implementation Guidelines upon acceptance by the RIS Committee together with the date when these changes will enter into force.

7.5 Dispute Resolution

Any dispute arising out of or in connection with this Agreement, including any question regarding its existence, validity or termination, shall be referred to and finally resolved by the arbitration of the RIS Committee,