

# **Assessing the legal framework behind Finland's PortNet\***

This study examines legal issues relating to establishing and functioning of a national port information community system in Finland operated by the Maritime Administration, customs and the largest ports in the country as a "single window" mechanism"

**\* This case study has been prepared by Teemu Puutio, LL.B. under the guidance of Yann L. Duval, Acting Chief, Trade Facilitation Section, ESCAP. The case study has also benefitted from the insights and comments of Mr. Antti Arkima, expert at the Finnish Transport Agency and Mr Luca Castelliani, legal office at UNCITRAL. For questions and comments on the specific details of the case, readers may write an email to [duvaly@un.org](mailto:duvaly@un.org)**

Summary .....	1
Beneficial categorizations when examining SW's.....	2
A source checklist for conducting legal research on the legal basis of a SW .....	3
When conducting legal research on the legal basis of a SW .....	5
1. Introduction .....	7
2. Generally on the legal framework behind PortNet .....	9
2.1. The first decade and the current situation .....	9
2.2. The directly applicable legal framework after May 2012 .....	10
2.3. The general international legal framework .....	12
3. The enabling legal Framework behind PortNet.....	13
3.1. Data authenticity .....	14
3.2. Data protection and data privacy .....	16
3.3. Access to data .....	16
3.4. Media neutrality .....	17
3.5. Intellectual property, liability and other issues .....	18
3.6. Exchange of data.....	18
4. In conclusion .....	20
5. References .....	22

## Summary

Single Windows (SW) form an integral part of the modern day trade facilitation arsenal. Today it is almost self-evident that the use of electronic data interchange methods (EDI) in e.g. customs clearing and export/import related notifications can significantly reduce non-tariff trade barriers and confer tangible benefits to the trading community.<sup>1</sup> Early movers like Singapore have been able to enjoy of such benefits for more than decades, showing the way for countries like Lao People's Democratic Republic which have only recently begun taking concrete steps towards establishing SWs. Finland's journey towards establishing its own SW, PortNet, begun already in the 1990's. After almost a decade of determined planning, coding and testing the maritime trade related SW was launched in 2000. PortNet is a true one-stop-shop for those involved in maritime trade and it caters to the varying needs of private operators and local authorities by maintaining ship time tables, cargo information, statistical data on ships that have visited Finnish ports, service orders information, fairway payment data and other various drop-down tables and statistics. Since its launch PortNet has drastically reduced the need to fill and process paper forms. Today over 99% of the overall maritime traffic from and to Finland is now been processed electronically through the SW.<sup>2</sup>

A key learning to take away from the Finnish experience is that efficient SW systems can be created in a rather effortless and streamlined manner as long as there is enough governmental support and political will. The success story of PortNet proves that a SW system can largely rely on the legal framework which enables the operations of information society services on a more general level without the need for specifically establishing provisions. In fact, it is clear that only a few specific provisions in secondary legislative instruments are sufficient to enable the SW's functioning. However, it seems

---

<sup>1</sup> UN/CEFACT Recommendation 33

<sup>2</sup> Bäckström 2006.

to be necessary to have a previously established and comprehensive legal framework concerning the legal status of electronic communications, their equivalence with paper documents, electronic signatures, and privacy and data retention.

### **Beneficial categorizations when examining SW's**

In the context of trade facilitation through SWs one of the most interesting research questions is simple: how was the SW implemented? The reason why this question is of such interest is that SWs can be established in multifarious manners. As presented already in the UN/CEFACT Recommendation 33, there is a range of different models for the implementation of a SW ranging from so called *single authority* approaches to *automated information transaction systems*. The various models differ e.g. with respect to how the EDI systems are connected and by whom they are operated. It is natural that the practical measures taken by each SW implementing nation vary. However, it is commonly expected that these measures include some form of legislative or regulatory actions. From here we can approach perhaps an even more interesting yet more complex question: what is the legal basis and backgrounds of the SW?

SWs can be subject to a plethora of various legislative or regulatory instruments and rules covering the full spectrum from court precedents to acts passed by the parliament or even the constitution. Further examination of the legal basis of a SW brings us to realize that there is a distinct categorization of existing norms into so called directly and in-directly enabling norms. These two categories share a common feature insofar as they both play a role in making the SW's operations legally possible. However, there is a distinct need to examine them separately because of the differences in their scope and aim: Whereas directly enabling norms are specific instruments enabling the SWs operations indirectly enabling norms can cover larger plots like the use of electronic signatures in all electronic communications for instance. Another necessary categorization is the division of norms applicable to the SW's operations into national and international norms. This division is important partly because of the need to fully

understand the legislative and political processes which underlie the legal basis of a SW. The categorization also provides a way to examine the SW's interconnections to the multinational forum of trade related law.

### **A source checklist for conducting legal research on the legal basis of a SW**

When approaching SWs from a legal perspective it is necessary to be aware of the separate sources of law and their distinctions. The first and most important sources for directly enabling norms are so called *primary legal sources*. Such sources cover all parliament enacted laws including acts, statutes and the constitution. In addition other legal instruments like ministerial orders and decrees promulgated by a government authority having the right to do so are to be held as primary legal sources. Possibly applicable administrative decisions and binding court precedents must be taken into account as well. The main focus of the legal research should be within these primary sources which make up the majority of directly and indirectly enabling norms. Once the primary sources have been exhaustively assessed it is necessary to assess the existing *secondary legal sources*. Such sources should be first and foremost used in order to provide resources for further analysis and interpretation of the primary legal sources. Whereas these sources including e.g. white papers, reports and government bills are not on an equal standing with the primary sources their importance can be all but similar in situations where primary sources are scarce or non-existent. A final source for legislative materials is the category of so called *soft legislation*. This category includes materials like existing interpretations, commentaries and opinions which can be beneficial for conducting the legal research. In addition to purely legal materials it is also necessary to examine other materials that affect the operations of an SW. Such materials include e.g. national policies, contract law arrangements and international standards.

## Source checklist

1. Primary sources including:
  - National laws (acts, statutes, decrees, etc.)
  - Decisions and orders (Ministerial decrees, Regulatory authority orders, etc.)
  - Binding court precedents
  - International laws, agreements, treaties etc.
  
2. Secondary sources including:
  - Laws (acts, statutes, decrees, etc.)
  - Decisions and orders (Ministerial decrees, Regulatory authority orders, etc.)
  - Binding court precedents
  - Binding international body decisions
  
3. Soft legislation
  - Legal reviews
  - Existing legal interpretations
  - E.g. Special Rapporteur opinions
  
4. Other materials
  - International standards
  - National policies
  - Contractual arrangements

Today, many countries which have existing SWs usually allow for rather effortless access to the sources mentioned above. Existing legislation can often be accessed through centralized databanks like in the case of Finland and Singapore. Said countries also uphold a SW specific website from which the various other sources and the relevant authorities can be reached easily. If no such depositories exist it might be necessary to

attempt to contact the authority responsible for the SWs operations in order to obtain access to the relevant sources. At minimum, contacting the relevant authority is necessary in order to obtain information on the contractual arrangements concerning the SW, including end-user-license-agreements.

### **A subject matter checklist for conducting legal research on the legal basis of a SW**

When conducting legal research on the legal basis of a SW the sources listed above can be effectively examined with in a two-step process. First, in order to uncover the directly enabling normative framework, the sources can be filtered in search of direct references to the national SW. A valid approach is to look for mentions of the specific name of the SW or its method of implementation. After this it is suggested to search for the explicit operations the SW is responsible for and the modalities concerning it. In the case of Finland, such a search will return e.g. Section 20 of Act on Vessel Traffic Service (623/2005) which states that the *“the Vessel Traffic Services authority shall establish and upkeep a national seafaring information management system.”* This provision is a quintessential directly enabling provision for PortNet. Other provisions that can be found this way include several Customs Decrees which describe the operations PortNet is responsible for. As is the case with PortNet, there might not be an abundance of normative materials that have references to the SW itself. This is because an SW can be established and operated without it relying on directly enabling legislative instruments but rather on the efforts and certain authorities and the existence of a consensual politic will.

The second step entails taking a wider look at the existing legal sources in search for materials covering essential issues for an SW such as media neutrality documents and electronic signature norms. The fact that the majority of the issues which enable an SW also enable electronic commerce in general alleviates the burden on the researches due

to a relative cornucopia of existing research. The issues that are of interest and most likely involved in the enabling normative framework are listed in the checklist below.

A minimum checklist concerning the subject matter

**Step 1**

1. SW specific norms
2. Customs procedures related legislation and regulation

**Step 2**

3. Electronic signatures
4. Electronic documents
5. Data integrity
6. Data exchange and access to data
7. Data privacy and data protection
8. Data retention, archiving and use of data as evidence
9. Intellectual property
10. Dispute settlement
11. Competition law
12. Mutual recognition and other cross-border issues pertaining to the SW's operations

Regardless of whether the norms concerning the issues mentioned above are directly referencing the SW in question they are key components in establishing the overall network of enabling norms that ultimately allow the SW to operate. In the case of PortNet the majority of enabling norms were found in generally applicable legislative instruments which prescribe e.g. the use of electronic signatures in all circumstances, including the operations of the SW.

## 1. Introduction

This case study focuses on the legal framework behind the success story of PortNet; the Internet-based business-to-government Single Window (SW) used by private operators and government authorities involved in maritime trade traffic in Finland. The entities taking advantage of the SW include the Customs, Port Authorities, ship agents, stevedoring companies, vessel traffic operators, the Maritime Administration and the Finnish Frontier guard.<sup>3</sup> PortNet provides the necessary basic functionalities of a maritime trade SW system including cargo manifest processing, customs clearance in accordance with the European Import Control System procedures and the maintenance of shipment databases in accordance with the International Maritime Organization's International Convention for the Safety of Life at Sea.<sup>4</sup> The system also caters to the varying needs of private operators and local authorities by maintaining ship time tables, cargo information, statistical data on ships that have visited Finnish ports, service orders information, fairway payment data and other various drop-down tables and statistics (cf. Figure 1).<sup>5</sup>

PortNet was first launched in 2000, almost a decade after the process to create a national SW system which would streamline the previously burdensome procedures related to maritime trade was initiated. Prior to PortNet's implementation there were more than 6 paper forms that were required to be manually completed at port arrivals and departures.<sup>6</sup> In addition to being numerous, the forms were often redundant as an approximate 80% of the contents were identical.<sup>7</sup> PortNet has drastically reduced the need to fill and process paper forms and as of after 2006 over 99% of the overall

---

<sup>3</sup> Shortsea Promotion Centre Finland 2012

<sup>4</sup> Bäckström 2006

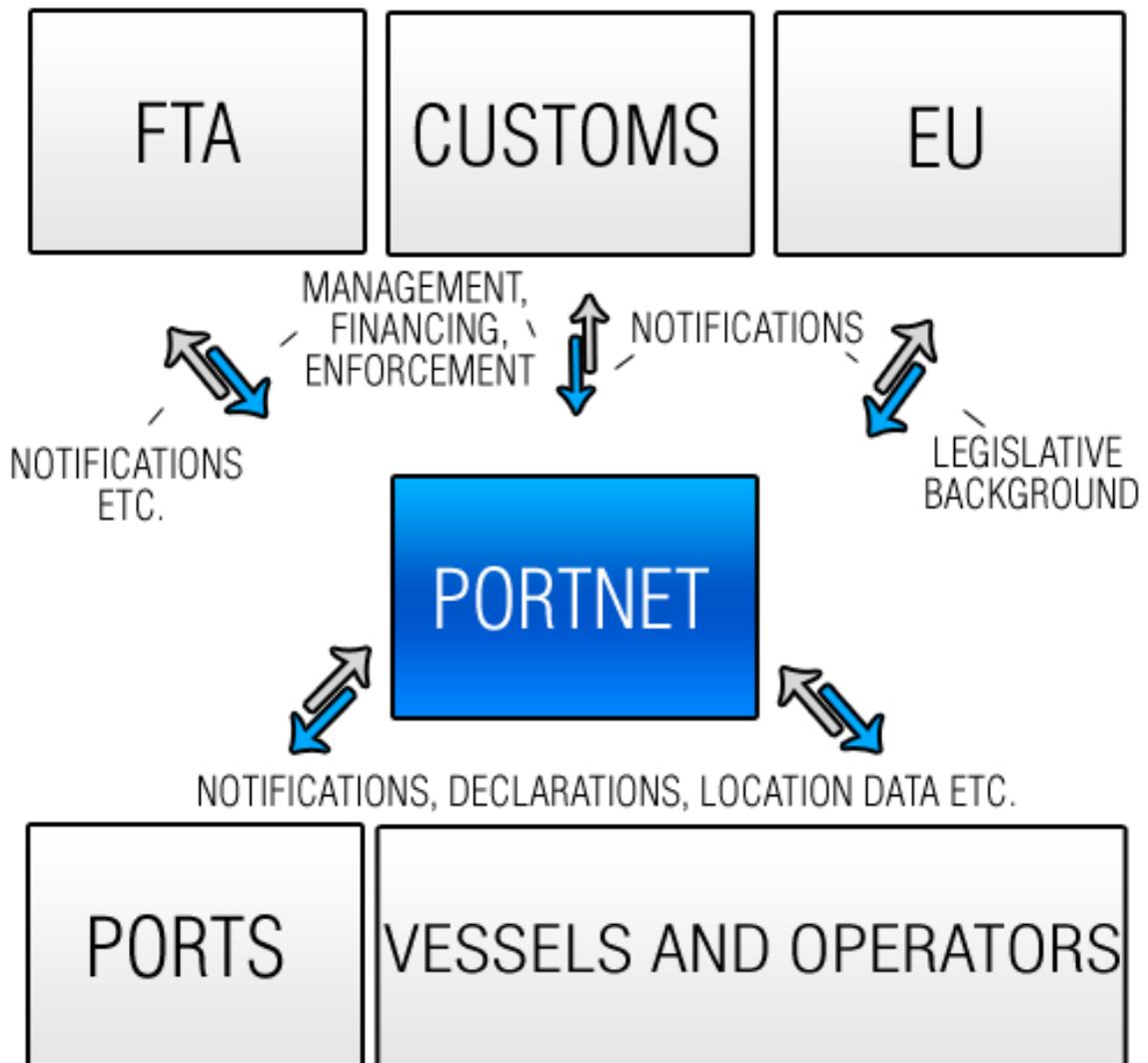
<sup>5</sup> Leviäkangas – Hautala 2002

<sup>6</sup> Suvila 2007.

<sup>7</sup> *ibid.*

maritime traffic from and to Finland has been processed via the SW.<sup>8</sup> As of October 2009 using PortNet has been obligatory, and today the service has approximately 1000 unique users daily.<sup>9</sup> All in all, PortNet handles over 40 000 port call notifications and 70 000 cargo declarations per year. Currently the service is operated and managed by the Finnish Transport Agency (FTA). In addition to the FTA also the Finnish Customs take part in managing and financing PortNet.<sup>10</sup>

**Figure 1: PortNet operational structure**



<sup>8</sup> Bäckström 2006.

<sup>9</sup> Finnish Transportation Agency 2012

<sup>10</sup> Suvila 2007

## **2. Generally on the legal framework behind PortNet**

### ***2.1. The first decade and the current situation***

Firstly, it is important to note that PortNet was not originally established by means of legislation. During the first nine years of its operations (2000-2008) PortNet was a community that was operated by Finnish Maritime Administration (FMA), the Customs and twenty of the largest ports in Finland. PortNet was essentially established on a need-driven basis by one single authority, namely the FMA which also took responsibility of its development and initial financing. Thus, the SW system itself was established and implemented without mentionable legislative efforts. Even after the first legislative instruments concerning PortNet were set forth the legislative framework was kept light and flexible: until 2009 PortNet was indirectly affected by the act concerning the Finnish Maritime Administration and after 2009 PortNet was also affected by the act regarding the Finnish Transport Agency.

In the first decade the only direct provisions concerning PortNet had been set forth in Customs decree 155/010/03 (later amended by decree 152/010/09), which is the instrument with which the Customs has implemented nationally Directive 2002/6/EC concerning the reporting formalities for international trade. Said decree obligates vessels to use PortNet for various notification purposes. The decree does allow for the use of alternative notification delivery methods however, in anticipation of potential service cut-offs or other issues pertaining to the availability of the electronic SW service.

Currently PortNet's operations are also affected by Customs decrees 23/010/2010, 152/010/09, 184/010/09, 26/010/07, 200/010/07 and 193/010/05. Said decrees mostly concern the procedural aspects of information provided to Customs e.g. as follows.

Customs decree 152/010/09<sup>11</sup>

*Paragraph 2*

*The notification of a vessels arrival must be placed in PortNet within an hour of the ships arrival [...]*

*[...] If the notification is not given through PortNet it shall be submitted with form 1s-09 via email or fax to MEKE.*

## **2.2. The directly applicable legal framework after May 2012**

The aforementioned situation will be changed in May 2012 when the European Directive on reporting formalities 2010/65/EU will be implemented by an amendment on the Act on Vessel Traffic Service (623/2005). The amendment adds an obligation for the FTA to establish and upkeep an electronic SW-system, namely PortNet, for the purposes of collecting maritime trade information regarding ships calling at Finnish ports (cf. Figure 2). The amended act and the accompanying Finnish Customs and Finnish Transport Agency decrees, which are unavailable at the time of writing, will come into force in 19.5.2012, which is also the official date for transposing the related directive. After the aforementioned date the Act on Vessel Traffic Service will contain the following provisions concerning PortNet :

Section 20 a<sup>12</sup>

*The Vessel Traffic Services authority shall establish and upkeep a national seafaring information management system in order to collect, process and record the information mentioned in the Directive on reporting formalities.*

---

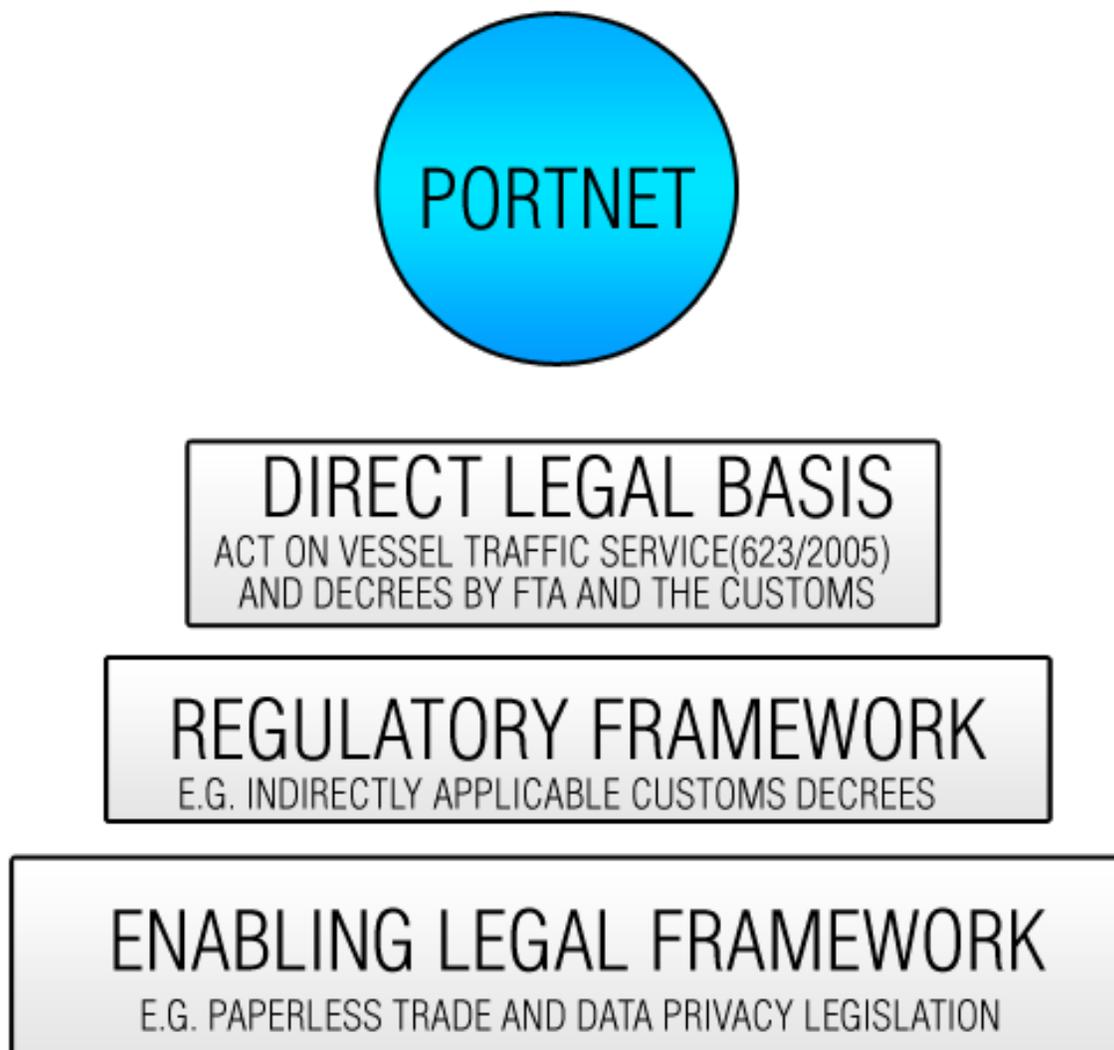
<sup>11</sup> Unofficial translation.

<sup>12</sup> Unofficial translation.

Section 22 a<sup>13</sup>

*The operator, agent of chief of any vessel arriving to a Finnish port or anchoring point shall send an electronic notification via the information management system referred to in Section 20 a.*

**Figure 2: PortNet national legal framework after 19.5.2012**



---

<sup>13</sup> Unofficial translation.

### **2.3. The general international legal framework**

The most significant international legislative instrument concerning PortNet is the International Ship and Port Facility Security (ISPS) Code which is an amendment to the Safety of Life at Sea (SOLAS) Convention (1974/1988). Said code sets forth obligations for various entities involved in maritime trade such as governmental authorities, shipping companies and ports involved in international trade and it aims to, *inter alia*, facilitate the detection of security threats and to strengthen preventive measures taken against security incidents affecting ships or port facilities. As Finland is a member of the European Union the legislation of the community create a significant legal framework for PortNet as well. Within the legal framework of the European Union the Directive 2010/65/EU on reporting formalities, Directive 2002/59/EC establishing a Community vessel traffic monitoring and information system as amended by 2009/17/EC, Directive 2009/42/EC on maritime statistics, Directive 2009/16/EC on Port State Control, Directive 2000/59/EC on Ship generated waste and cargo residues are all within the legal framework of the EU. However, the Directive 2010/65/EU on reporting formalities is perhaps the most significant directly applicable legislative instrument. In addition there are numerous significant and enabling directives such as the Directive on a Community framework for electronic signatures (1999/93/EC) and the Data Protection Directive (95/46/EC) which create the basis for the paperless trade environment. The international legal framework not only encompasses treaties or legislative instruments but also other forms of regulations such as international quality standards<sup>14</sup> used within the context of electronic signatures which have been recognized by the European Commission<sup>15</sup>. In addition, the international legal framework also incorporates soft-law instruments such as the UN/EDIFACT and UN LOCODE standards.<sup>16</sup>

---

<sup>14</sup> Said standards include e.g. CWA 14167-1, CWA 14167-2 and CWA 14169.

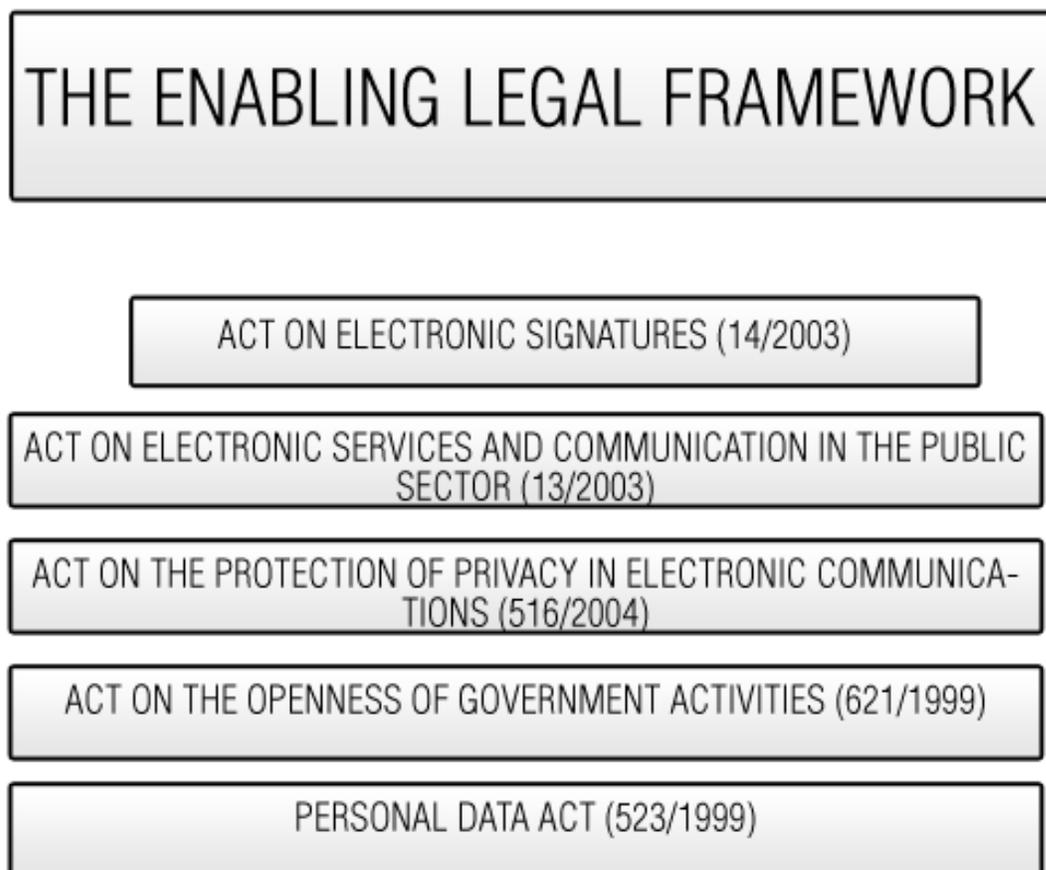
<sup>15</sup> Commission Decision no. 2003/511/EC of 14 July 2003.

<sup>16</sup> UNECE 2006

### 3. The enabling legal Framework behind PortNet

As mentioned above the legislative framework behind PortNet has been light and without substantive provisions concerning PortNet. The situation remains the same even after the amended Act on Vessel Traffic Service comes into force in mid-2012. However, the legal framework behind PortNet is rather complex and multifaceted because the service operates in the broader context of an enabling legislative environment made of comprehensive laws of general application (c.f. Figure 3).<sup>17</sup>

**Figure 3: An overview of the current enabling legal framework**



<sup>17</sup> Hautala, - Leviäkangas - Kulmala – Auvinen – Berglund 2003.

This enabling legal framework quite naturally includes the Customs Act (1994/1466) which sets forth general obligations pertaining to the Customs procedures and cross-border trade.. In addition to the Customs Act, the Act on Fairway Dues (1122/2005) enables the SW system by stipulating on key issues such as the electronic provision of information and the notification of payment procedures. Other, more significant, enabling acts include, amongst others, the Act on Electronic Signatures (14/2003) the Act on the Protection of Privacy in Electronic Communications (516/2004) the Act on the Openness on Government Activities (621/1999) the Act on Electronic Services and Communication in the Public Sector (13/2003). Said acts also lay down the general framework for paperless trade. The most significant legislative instruments are detailed further in this chapter in accordance with the general areas of the enabling legal framework.

### ***3.1. Data authenticity***

When moving from a paper-based business-to-government environment towards a paperless SW system, several issues concerning the security and authenticity of documents and information need to be dealt with. In order to ensure the integrity and authenticity of the documents provided within the system PortNet incorporates both legislative and technological approaches. However, as mentioned earlier, PortNet mostly relies on the common and pre-existing legal framework. Consequently, the legal instruments referred to here apply to all electronic communications in general. One of the most significant legal instruments safeguarding data authenticity is the Act on Electronic Signatures, which establishes the legal status of electronic signatures. Electronic signatures enjoy equal status with traditional signatures, and they can be used interchangeable e.g. within contractual frameworks.

### *Section 5*

*If the legal proceeding requires an signature to be fulfilled this requirement is met by, at least, by such a developed electronic signature which is based on a quality certificate and which as been created by a secure signature creation device.<sup>18</sup>*

The Act on Electronic Services and Communication in the Public Sector is also significant, as it includes provisions on using electronic signatures and documents when dealing with the public sector e.g. as follows:

### *Section 13*

#### *Notification for payment*

*The notification may also be submitted in electronic form or in another form suitable for data processing.*

### *Section 33*

#### *Electronic provision of information*

*The decision of the customs authorities may also be communicated in electronic form by using the address for electronic business given by the party liable to pay. In that case and unless proven otherwise, the decision is considered to have been received by the party liable to pay on the day the electronic message was sent.*

The aforementioned acts both enable the use of electronic signatures and documents and aim to safeguard the related data authenticity. In addition to taking advantage of the legal framework PortNet also uses internal practices and mechanisms which aim at ensuring the integrity and authenticity of data. For instance, the service can be accessed only after secure user authentication and after this the data is sent via dedicated data communication networks to PortNet. The internal mechanisms adhere to common international standards concerning electronic signatures, namely to those endorsed by the European Committee for Standardization.<sup>19</sup>

---

<sup>18</sup> Unofficial translation.

<sup>19</sup> European Committee for Standardization 2012

### **3.2. Data protection and data privacy**

Similarly to the above, a mixture of legal and technological measures is enforced in safeguarding a satisfactory level of data protection. The legal framework concerning data protection and privacy in Finland is extensive and rather fragmented as the relevant provisions are spread out over several legal instruments. A legal reform which will eventually provide a coherent and concise body of legislation has been under discussion for some time, but concrete results are not expected in the near future. Until then, provisions relevant to data protection are included in the Personal Data Act (523/1999) which stipulates on the use of personal information on a more general level. The act sets forth several basic requirements concerning how personal data can be managed, and for what reasons it can be used. As such the act is essentially a safeguard against misuse and misappropriation. In addition to the aforementioned, the Act on the Protection of Privacy in Electronic Communications is a significant legislative instrument with regard to data protection and privacy. Said act contains, *inter alia*, obligations on data secrecy and non-exploitation. Also the Act on the Openness of Government Activities must be noted in this context, as it sets down rules concerning access to and the publicity of official documents. Finally, also the Customs Act stipulates on the secrecy of information disclosed or discovered in the course of the Customs' operations.

### **3.3. Access to data**

As mentioned above, data protection and data privacy are also safeguarded via internal technical mechanisms which restrict access to data within the PortNet environment. User rights are assigned on a case-to-case basis and each user type has different rights to either add or review data placed into the SW system to varying extents. Basic users are authorized to access information related to their own activities and responsibilities and also any data which is made public within the system such as e.g. timetable data. This means *e.g.* that port authorities have access only to necessary

data for the operation of their own port and ship agents can access only information concerning them directly. Other user types such as Port authorities have limited access to information which directly concerns their related activities or obligations. In addition to the system operator, namely FTA, some other government authorities such as Finnish Customs and all authorities which are listed as surveillance authorities in Directive 2002/59/EC have extensive rights to review all data. Said user types are exclusively governmental authorities or state-owned entities. It must be noted that the governmental authorities or entities involved in PortNet are limited to those who have a direct and explicit need to access the information within PortNet established by standing legislation, as is the case with the Customs or the Frontier guard.

### ***3.4. Media neutrality***

It is worth noting that as a general rule Finnish legislation does not discriminate between electronic and hard-copy documents when dealing with government authorities. In addition, the use of electronic methods of distribution and information exchange is strongly encouraged by the Finnish legal framework. Within the PortNet SW context the use of electronic media is specifically preferred as Customs decree 155/010/03 (as amended by 152/010/09) states that the necessary notifications must be sent via PortNet electronically. However, the decree is in essence media neutral, as it does allow for notifications via email, paper forms and faxes as an alternative for PortNet. The media neutrality is limited however, and the flexibilities are meant facilitate the transition to a paperless environment and to not create unnecessary barriers affecting operators that do not have access to online services. Also some other Customs decrees, which were mentioned earlier, either directly obligate or strongly prefer electronic submitting of information and notifications.

### **3.5. Intellectual property, liability and other issues**

Establishing SW systems can bring up potentially problematic issues concerning the ownership of intellectual property rights. This is mostly because SW systems require use of software, extensive databases and confidential information which fall under the protection of intellectual property rights. The fact that Finland upholds a strong level of intellectual property rights helps deter possible problematic situations to some extent. All in all, intellectual property issues are unlikely to disrupt PortNet's operations, partly because the software and all related intellectual property rights have been created and are owned by state-owned entities. Because of this control over the proprietary intellectual property rights the threat of third party injunctions or other forms of disruptions is minimized.

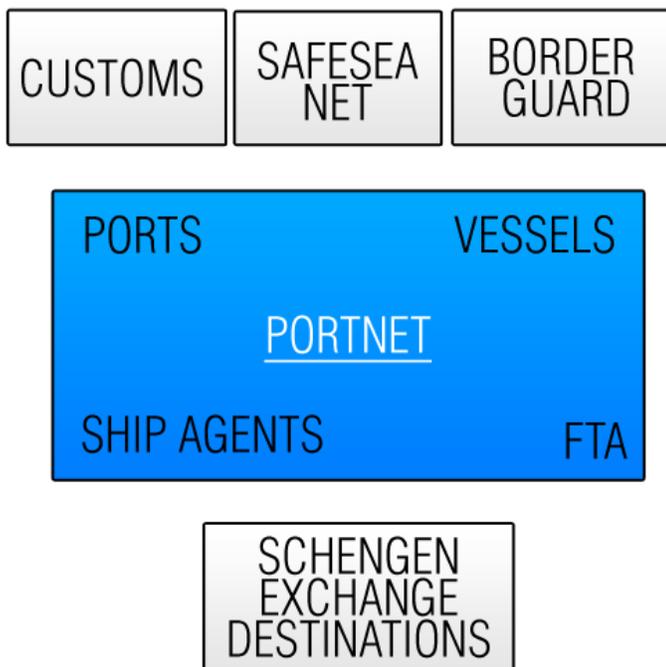
### **3.6. Exchange of data**

In general, data and information is exchanged with other authorities *in casu and* on a need-to-access basis (cf. Figure 4). Exchange of data provided to the PortNet system within national governmental authorities is regulated in part by the Customs Act and partly by Directives 2002/59/EC, 2010/65/EU and 2009/42/EC as implemented by the Act on Vessel Traffic services. The Customs act allows the Customs to provide relevant authorities such as the Police and the Border Guard with any information necessary for said authorities to fulfill their law enforcement duties. When information is exchanged the Customs must take the necessary measures to ensure the protection of personal data and the authority responsible for the data exchange must also take into account the relevant provisions of the Convention of the Council of Europe of 28 January 1981 for the protection of individuals with regard to automatic processing of personal data and the provisions of the Convention concerning the use of information technology for customs purposes.<sup>20</sup>

---

<sup>20</sup> [http://europa.eu/legislation\\_summaries/customs/133051\\_en.htm](http://europa.eu/legislation_summaries/customs/133051_en.htm)

**Figure 4: Exchange of data within the PortNet context**



PortNet also allows for information to be exchanged internationally. At current, PortNet provides direct input to the SafeSeaNet system without involving any intermediate operators.<sup>21</sup> It is also due noting that as a member of the European Union Finland is and has been actively involved in the integration process related to Customs operations and thus data and information submitted to PortNet are subject to data exchange procedures in accordance with the essential agreements of the integration. Notable instruments concerning such data exchange include *e.g.* the Schengen agreements which concern cross-border co-operation and data exchange. Also, Finland has implemented the Council Framework Decision 2006/960/JHA of 18 December 2006 on simplifying the exchange of information and intelligence between law enforcement authorities of the Member States of the European Union. Thus information provided to PortNet can be exchanged internationally as is necessary within the set regulations.

---

<sup>21</sup> Suvila 2006

#### **4. In conclusion**

The direct and enabling legal framework detailed in the previous chapters has been largely influenced by EU legislation. For instance, the currently standing legal instruments concerning data privacy issues and electronic signatures incorporate national implementations of EU directives. In addition various supra-national legislative instruments such as the ISPS and their respective development processes have influenced the legislative framework behind PortNet. Thus, the development process behind the general legal framework has been international to a large extent. However, the implementation is uniquely Finnish and a result of the efforts of various ministries such as the Ministry of Transportation and Communication. Thus, the development process behind the directly applicable legal framework is a mixture of both national and international contributions.

The success story of PortNet shows that a SW system can largely rely on the legal framework which enables the operations of information society services on a more general level without the need for specifically establishing provisions. The Finnish experience shows that efficient SW systems can be created in a rather effortless and streamlined manner as long as there is enough governmental support from *e.g.* the participating authorities. As a precedent PortNet, proves that a comprehensive legislation allowing paperless trade and information exchange and safeguarding data authenticity and data protection is sufficient to enable the seamless operation of a business-to-government SW system (see Figure 4). In conclusion, the experience of PortNet proves that a few specific provisions in secondary legislative instruments are sufficient to enable the SW's functioning provided that a comprehensive legal framework on the legal status of electronic communications, their equivalence with paper documents, on electronic signatures, and on privacy and data retention, *inter alia*, are already in place (cf. Figure 5).

**Figure 5: Essential components for an enabling legal framework**



## 5. References

### *Literature*

Bäckström, R. (2006) "Single Window Implementation. Experience of Finland. Symposium on Single Window Standards and Interoperability, United Nations Economic Commission for Europe 3-5 May, Geneva.

UNECE (2006) "Case Studies on Implementing a Single Window to Enhance the Efficient Exchange of Information", Geneva.

Leviäkangas, P., Hautala, R. (2002)" Impact evaluation of maritime I.T.S – Case PortNet", Finland.

Hautala, R., Leviäkangas P., Kulmala, R., Auvinen, S., Berglund, R (2003) "PortNet Impact Evaluation". FITS Publications 15/2003. Finland: Helsinki.

### *Online*

Shortsea Promotion Centre Finland 2012,  
[http://www.shortsea.fi/index.php?option=com\\_content&task=view&id=57&Itemid=49&lang=en](http://www.shortsea.fi/index.php?option=com_content&task=view&id=57&Itemid=49&lang=en) (accessed 22 January 2012)

Finnish Transportation Agency 2012, <http://portal.liikennevirasto.fi/sivu/www/portnet> (accessed 22 January 2012)

Finnish Communications Regulatory Authority 2012,  
<http://www.ficora.fi/en/index/saadokset/lait/sahkoinenallekirjoitus.html> (accessed 22 January 2012)

European Committee for Standardization 2012,  
<http://www.cen.eu/CEN/sectors/sectors/iss/cen%20workshop%20agreements/Pages/electronic%20signatures.aspx> (accessed 22 January 2012)