ELECTRONIC SINGLE WINDOW LEGAL ISSUES

A CAPACITY- BUILDING GUIDE

UNNExT
United Nations Network of Experts for Paperless Trade in Asia and the Pacific

UNITED NATIONS ESCAP
Economic and Social Commission for Asia and the Pacific

UNECE
United Nations Economic Commission for Europe

The United Nations Economic and Social Commission for Asia and the Pacific (ESCAP) is the regional development arm of the United Nations and serves as the main economic and social development centre for the United Nations in Asia and the Pacific. Its mandate is to foster cooperation between its 53 members and 9 associate members. ESCAP provides the strategic link between global and country-level programmes and issues. It supports Governments of countries in the region in consolidating regional positions and advocates regional approaches to meeting the region's unique socioeconomic challenges in a globalizing world. The ESCAP office is located in Bangkok, Thailand. Please visit the ESCAP website at www.unescap.org for further information.

The darker area of the map represents the members and associate members of ESCAP

The United Nations Network of Experts for Paperless Trade in Asia and the Pacific (UNNExT) is a community of knowledge and practice for experts from developing countries and transition economies from Asia and the Pacific involved in the implementaation of electronic trade systems and trade facilitation. Established by ESCAP and the United Nations Economic Commission for Europe (UNECE), UNNExT aims to support national, subregional and transcontinental Single Window and paperless trade initiatives. It's emphasis is on training, knowledge sharing and application of international standards for trade facilitation. For more information on UNNExT, please visit www.unescap.org/unnext.

United Nations Network of Experts for Paperless Trade in Asia and The Pacific
United Nations Economic and Social Commission for Asia and The Pacific
United Nations Economic Commission for Europe

Electronic Single Window Legal Issues: A Capacity-Building Guide

UNNExT
United Nations Network of Experts for Paperless Trade in Asia and the Pacific

UNITED NATIONS ESCAP
Economic and Social Commission for Asia and the Pacific

UNECE
United Nations Economic Commission for Europe

Electronic Single Window Legal Issues: A Capacity-Building Guide

United Nations publication

Manufactured in Thailand

ST/ESCAP/2636

The designations employed and presentation of the material in this publication do not imply the expression of any opinion whatsoever on the part of the secretariat of the United Nations concerning the legal status of any country, territory, city or area or of its authorities, or concerning the delimitation of its frontiers or boundaries.

Disclaimers

The opinions, figures and estimates set forth in this publication are the responsibility of the authors, and should not be considered as reflecting the views or carrying the endorsement of the United Nations or of UNNExT members or partners.

Mention of specific names and commercial products and services does not imply the endorsement of the United Nations.

Foreword

Developed and developing countries alike are increasingly engaged in the development of paperless trading systems, often as part of broad based e-government or trade competitiveness initiatives. Computerized or automated customs systems are already in place in almost every country, including many of the least developed and landlocked developing economies. Governments are now going further, as they realize that replacing only some of the paper documents involved in a trade transaction by electronic ones may not yield the intended benefits. Therefore, they are actively working on the development of electronic single windows to provide a unique national platform through which all trade transaction information can be communicated by traders to all regulatory agencies.

To ensure that these paperless trading platforms can operate and ultimately replace paperbased systems, it is essential that an enabling legal framework be put in place. Development of such a legal framework can take time as new laws may need to be passed and existing laws may need to be amended. Single Window planners and decision makers, therefore, need to understand and start thinking about potential legal implications early on. In that context, this UNNExT Guide on Electronic Single Window Legal Issues is an important addition to the existing set of UNNExT guides and tools which have essentially focused on technical aspects of single window development, such as the Business Process Analysis Guide to Simplify Trade Procedures, the Guide for Alignment of Trade Forms, and the Data Harmonization and Modelling Guide for Single Window Environments.

It is our hope that this new *Guide* will respond to the need of government officials in charge of implementing single windows, many of whom may have a limited legal background. It is also our hope that this *Guide* and the application of the principles it promotes will contribute to the development of more harmonized paperless-trade legal frameworks across countries and ultimately facilitate cross-border paperless trade.

Ravi Ratnayake
Director
Trade and Investment Division
ESCAP

Virginia Cram-Martos
Director
Trade and Sustainable Development Division
UNECE

Acknowledgements

This publication was prepared under the guidance of Ravi Ratnayake, Director, Trade and Investment Division (TID), ESCAP by a team consisting of William J. Luddy, UNNExT Legal Advisory Group Member and Special Legal Counsel to the World Customs Organization, Yann Duval, Acting Chief, Trade Facilitation Section, TID and Teemu Puutio, Legal Research Assistant, Trade Policy Section, TID. Substantial substantive contributions were also received from Luca Castellani, United Nations Commission on International Trade Law (UNCITRAL), Rolf Weber, Professor of Law, University of Zurich, and Hong Xue, Professor of Law and Director of Institute for the Internet Policy & Law (IIPL), Beijing Normal University, China. Documents from the USAID Project on the ASEAN Single Window provided valuable input for the preparation of the legal analysis mini case studies. Also, the World Customs Organization, in particular Lee Sang-Hyup and Satya Prasad Sahu, provided valuable inputs.

The publication benefited from a peer review and comments by participants of the UNNExT Advisory Group Meeting on Legal Issues, held in Bangkok on 22-23 March 2012, including: Claro V. Parlade, Google Legal Counsel, Singapore; Pavan Duggal, Advocate, Supreme Court of India and President, Cyberlaw Asia; and Chong Kah Wei, Deputy Senior State Counsel, Legislation & Law Reform Division, Attorney-General's Chambers, Singapore; and from comments received on an earlier version of the Guide during an initial peer review meeting held in Bangkok on 26 July 2011, from: Harry Tan Soo Kiat, Associate Professor of Law, Nanyang Business School, Singapore; Sok Siphana, Siphana and Associates, Cambodia; and Markus Pikart, UNECE.

The peer reviewers participated in their individual capacity and any errors in the *Guide* are the responsibility of the authors.

Preface

The necessity of creating an enabling legal infrastructure has emerged as a critical element for the success of a Single Window (SW) facility at the national level and, to the extent possible, as a predicate for a harmonized approach at the regional and international levels. The extent to which trade facilitation can be achieved through the operation of a SW nationally and across borders indeed depends on the legal environment in which relevant stakeholders served by the SW, as well as those along the international supply chain, operate.[1] This legal environment, therefore, includes not only the Single Window enabling law at the national level but also the legal framework for electronic transactions that will provide a foundation on which the electronic Single Window will be operating. In this context, it is important to identify the essential legal issues related to the creation and operation of a single window in order to fully understand what types of legal gaps exist in national laws. This also presents an opportunity to consider how the technical architecture[2] of the single window can affect the range of legal issues that must be addressed. This exercise is useful to both governments that have already set up or are in the process of establishing SWs, particularly in locations where facilitating cross-border transactions would be a key benefit.

This *Guide* covers the wide-ranging legal issues that are related to the development and operation of a SW and, to a certain degree, some of the important electronic commerce legal concepts and approaches applicable to the single window environment. It is intended to give policymakers a broad understanding of the key considerations that should be addressed in effectively establishing the legal infrastructure for a SW. The *Guide* is not specifically aimed to be a resource strictly for lawyers but rather to those who are expected to drive the successful development of single window and paperless trade initiatives in their countries.

Many of the legal issues discussed in this *Guide* are generic to the legal infrastructure for both SW development and cross-border (or international) single window transactions as there can be substantial overlap between them. Therefore, as part of enabling the SW in national law, the Guide stresses the need for countries to adopt international legal standards to ensure as far as possible that the SW is interoperable, from a legal perspective, with other national and regional single window facilities.

Against this backdrop, the *Guide* examines the processes that can be employed to identify and assess those potential gaps in domestic law that would create barriers: (1) to the full operation of an electronic SW; (2) to the cross-border legal interoperability of electronic SWs; and (3) to the legal interoperability of the SW with non-governmental entities that will participate in the SW and electronic commerce transactions (domestic and cross-border). It also examines the essential legal elements that make up the areas of law that should be considered, as well as some of the organizational considerations that go into creating a SW. Furthermore, it aims to equip legal experts and policymakers with an appropriate and effective methodology for conducting the legal gap analysis as a key step in developing the national legal framework for a SW.

This *Guide* was developed based on the United Nations Centre for Trade Facilitation and Electronic Business (UN/CEFACT) Recommendation 33[3] and Recommendation 35,[4] the conventions and

[1] See, Schermer, Bart "Legal Issues of Single Window Facilities for International Trade," UNCITRAL Congress Modern Law for Global Commerce (July 2007).

[2] Chong, K.W., "Legal and Regulatory Aspects of International Single Window Implementation: The ASEAN Experience", Global Trade and Customs Journal, 4, pp. 185–193 (Kluwer Law International, 2009).

[3] UN/CEFACT Recommendation 33 – Recommendation and Guidelines on establishing a Single Window to Enhance the Efficient Exchange of Information between Trade and Government (July 2005).

[4] UN/CEFACT Recommendation 35 – Establishing a Legal Framework for the International Trade Single Window (2010).

model laws of the United Nations Commission on International Trade Law (UNCITRAL),[5] the international texts and work at the World Customs Organization (WCO) as well as the experiences and best practices that have emerged from the work done by governments, various United Nations organizations, and intergovernmental organizations (IGOs) and non-governmental organizations (NGOs) at the national, regional and international levels over the past eight or more years. It is the first edition of a living document that is expected to evolve as new legal standards and instruments continue to develop in the dynamic field of paperless trade and electronic commerce.[6]

[5] The UNCITRAL international texts and guidance documents related to electronic commerce are available at http://www.uncitral.org/uncitral/en/uncitral_texts/electronic_commerce.html

[6] Revised and updated online versions of this and other UNNExT capacity-building tools and guides are available at: http://www.unescap.org/unnext/

Content

List of Figures

List of Boxes

List of Acronyms and Abbreviations

ADR	alternative dispute resolution
AES	advanced electronic signature
APEC	Asia-Pacific Economic Cooperation
ASEAN	the Association of Southeast Asian Nations
ASW	ASEAN single window
B2B	business-to-business
B2C	business-to-consumer
B2G	business-to-government
CA	certification authorities
ECC	United Nations Convention on the Use of Electronic Communications in International Contracts, 2005
EDI	electronic data interchange
eID	electronic identity
ESCAP	United Nations Economic and Social Commission for Asia and the Pacific
EULA	end-user license agreements
G2C	government-to-citizen
G2G	government-to-government
GATT	General Agreement on Tariffs and Trade
ICT	information and communications technologies
ICTPA	the Mongolian Information Communications Technology and Post Authority
IPR	intellectual property rights
ISA	information security agreements
ISAs	interconnection security agreements
KCS	Korea Customs Service
LWG	legal working group
MOU	memoranda of understanding
MRA	mutual recognition agreements
OECD	Organization for Economic Development and Cooperation
PII	personally identifiable information
PIN	personal identification numbers
PKI	public key infrastructure
PPP	public-private partnerships
QES	qualified electronic signature
SEZ	special economic zone
SLA	service level agreements
SW	(electronic) single window
UN/CEFACT	United Nations Centre for Trade Facilitation and Electronic Business
UNCITRAL	United Nations Commission on International Trade Law
UNECE	United Nations Economic Commission for Europe
VNSW	Viet Nam single window
WCO	World Customs Organization
WTO	World Trade Organization

Part 1:
INTRODUCTION

A. The Single Window for Trade Facilitation

The concept of a *Single Window* (SW) to enhance trade facilitation is not entirely new. Efforts to simplify import, export and transit procedures have been underway for many years[7] and the idea of utilizing Information and Communications Technologies (ICT) emerged in the late 1970s. Electronic Data Interchange (EDI) was envisioned, for example, in 1979 when the Government of Singapore began its early discussions and work on what ultimately became its TradeNet system in 1989.[8]

Over the past 10 years, efforts to develop single windows have increased dramatically as a result of the growing importance of global supply chains in international trade. The concept of the SW for trade facilitation is not complex but implementation of the legal, technical and organizational aspects of a SW facility can be challenging. The United Nations Centre for Trade Facilitation and Electronic Business (UN/CEFACT) Recommendation 33 defines the SW as follows:

> ***A facility that allows parties involved in trade and transport to lodge standardized information and documents with a single entry point to fulfill all import, export, and transit-related regulatory requirements. If information is electronic, then individual data elements should only be submitted once.***

This definition is likely one of the most widely used descriptions of a SW facility. However, "Single Window" is not the only name that SW-type facilities have been called and some variants of the SW concept include, among others, a "one-stop-shop." In addition, similar SW-type approaches have been applied to other types of government services such as the "one-door-service" provided for in the Lao People's Democratic Republic foreign direct investment efforts.[9]

Work towards the ICT technical development of the Single Window in one form or another has been underway for well over 10 years. While using ICT is certainly not the only methodology for developing a Single Window,[10] an ICT approach has been emphasized in many national and international efforts. Additionally, the growing use of electronic commerce methods in international business transactions has demonstrated the increasing importance of ICT as a basis for Single Window operations. Organizations such as the United Nations Economic Commission for Europe (ECE),[11] the Economic and Social Commission for Asia and the Pacific (ESCAP)[12] and the World Customs Organization (WCO),[13] among others, have active programmes that focus on the general benefits and the technical aspects of paperless trade.[14]

[7] See e.g., the WCO's International Convention on the simplification and harmonization of Customs procedures (Kyoto Convention), entered into force in 1974.

[8] ESCAP, Trade Facilitation Handbook for the Greater Mekong Subregion (2002), pp. 51-53.

[9] Lao PDR Law on Investment Promotion, No. 02/NA, Vientiane, 8 July 2009. Article 44 describes the One-Door-Service as: "The investment's one-door-service is the services which provide the facilities in all fields to the investors through the provision of services on data and information, consideration of the investment, issuance of enterprise registration certificate or concession license and the issuance of notifications relating to the investment."

[10] As noted in UN/CEFACT Recommendation 33, "A Single Window does not necessarily imply the implementation and use of high-tech ICT, although facilitation can often be greatly enhanced if Governments identify and adopt relevant ICT technologies for a Single Window".

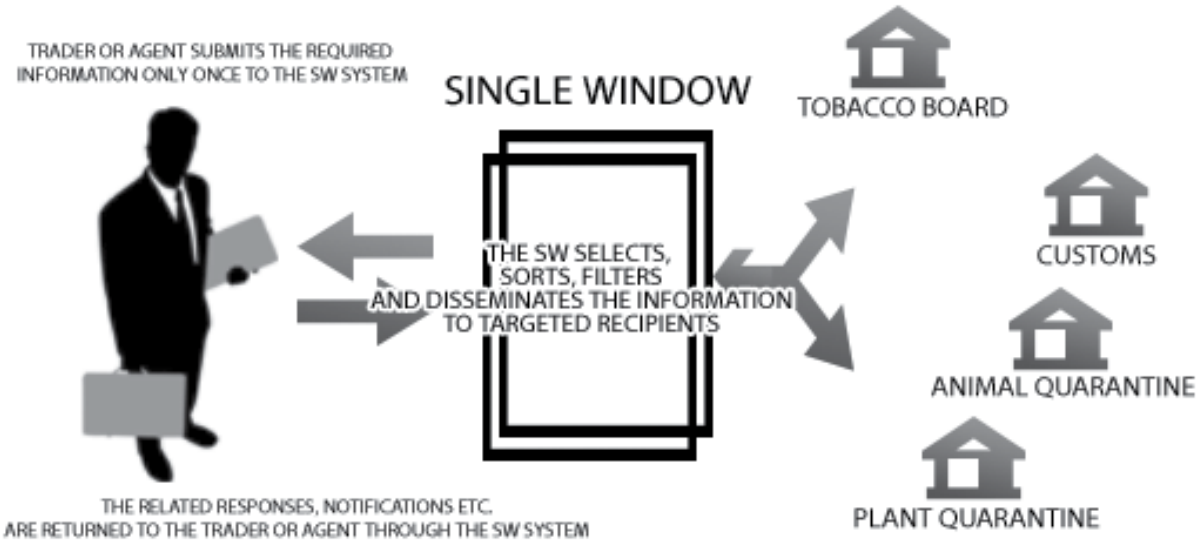
[11] Information on the UN/CEFACT that is part of ECE can be accessed at www.unece.org/cefact/

[12] For details, see UNNExT website at www.unescap.org/unnext/

[13] See, e.g., The WCO Data Model, available at http://www.wcoomd.org/

[14] See, e.g., "Workshop on International Standards to Stimulate Paperless Trade," Kuala Lumpur, Malaysia (20-21February 2006). These programs focus on the topic of "paperless trade" generally, within which the SW is an important component.

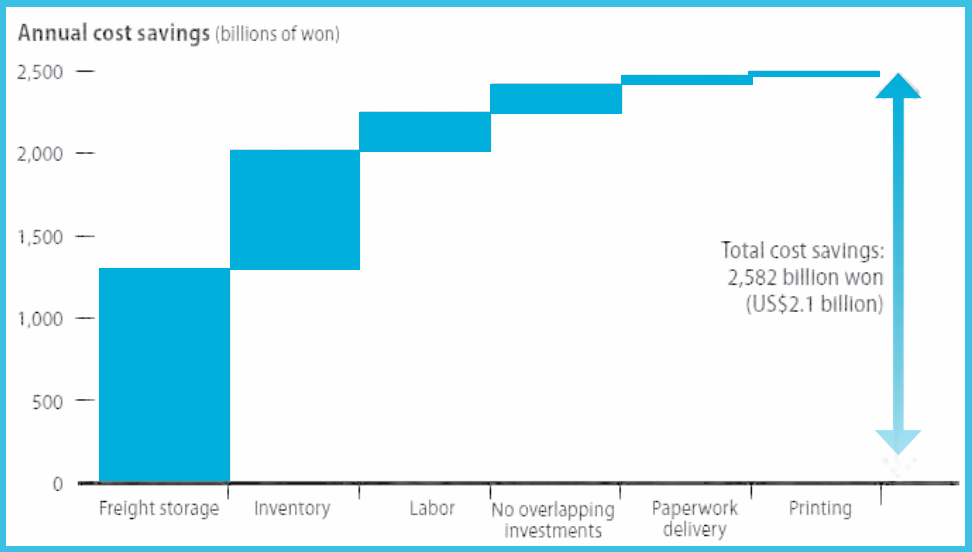
Figure I.1. Illustration of a Single Window Facility



BOX I.1. Benefits of creating a single window in the Republic of Korea

Republic of Korea Customs completed a single window system in July 2008, allowing traders, government agencies and private sector participants—including traders, banks, customs brokers, warehouse operators, carriers, insurance companies and freight forwarders—to exchange information in real time, thus speeding up approvals.

According to the World Bank's Doing Business report 2010, the Korea Customs SW system called UNI-PASS (http://portal.customs.go.kr), simplified the clearance process and reduced the clearance time, thus saving logistics cost and reducing the financial burden of the users by approximately $2 billion per year. In addition, UNI-PASS improved the quality of administrative service through reduction of data elements by sharing information through the Internet among the border agencies and other stakeholders.



Source: World Bank's Doing Business report 2010, p.52

Figure I.2. Alternative models of single window operations

Single Authority: A Single Authority that plays the role of a Single Window receives and disseminates information, and coordinates control for example, in the Swedish Single Window, the Customs Authority performs selected tasks on behalf of some authorities.

Single Automated System: A system that integrates the electronic collection, use and dissemination (and storage) of data related to trade that crosses the border, either on the territory of a whole country like PortNet in Finland or in one location like DAKOSY in Hamburg.

Automated Information Transaction System: A system that offers specific means of collecting incoming data. Through this system a trader can submit electronic trade declarations to the various authorities for processing and approving a single application. Approvals are transmitted electronically from governmental authorities to the traders' computer. Such a system is in use in Singapore and Mauritius.

Figure I.1. is one representation of a SW facility based, in part, on the definition contained in UN Recommendation 33 and incorporating a broader paperless trade perspective.

The benefits of national electronic single window systems are now well established. They typically include significant reduction in the time and overall cost of completing export/import procedures, as well as increased transparency. For example, the national single window of the Republic of Korea and related e-trade systems have brought enormous economic benefits through reduced labour and other costs associated with issuing and circulating documents, reduced costs of warehousing and inventory management, and reduced redundant investment in the IT sector (see Box I.1).[15]

Various approaches to a SW implementation model are possible. The best solution depends on compatibility with the local situation. For example, three common models described in UN/CEFACT Recommendation 33 are depicted in Figure I.2.[16]

Over time it is possible that other SW implementation solutions will emerge. The key is that SW should build as much as possible on existing international standards and best practices to ensure, as far as possible, interoperability with other SWs. From a legal perspective, that also includes ensuring that the SW facilities will comply with the current and future rules of the multilateral trading system negotiated at the WTO as well as the international standards emerging from the work of UNCITRAL in the area of electronic transactions.

FURTHER READING

"Recommendation and Guidelines on establishing a Single Window to Enhance the Efficient Exchange of Information Between Trade and Government", UN/CEFACT Recommendation No.33 (2005). Available at http://www.unescap.org/tid/unnext/tools/rec33_trd352e.pdf

"Recommendation on Establishing a Legal Framework for the International Trade Single Window to Enable the Development of Single Window Systems and Exchange of Information in the Single Window Environment", UN/CEFACT Recommendation No. 35 (2010).

Available at http://www.unece.org/fileadmin/DAM/cefact/recommendations/rec35/Rec35_ECE_TRADE_401_EstablishingLegalFrameworkforSingleWindow_E.pdf

[15] See The Case of Korea's National Paperless Trade Platform, *UNNExT Briefs on Towards a Single Window Trading Environment*, No. 3, 2010.
[16] See footnote n.4, UN/CEFACT Recommendation 33, p. 7-9.

Figure I.3. Building blocks towards a single window

Source: UNNExT, Towards a Single Window Trading Environment – Gaining Support from Senior-level Policymakers, Brief No. 1, November 2009.http://www.unescap.org/unnext/pub/brief.asp

B. The Intersection of Law and Technology in the SW Environment

Single window facilities are complex trade facilitation measures that require first and foremost strong political will in bringing the many stakeholders involved to work together towards a common system. Once the political will is there, establishment of stakeholder coordination mechanisms and the selection of a business model for the SW are often natural steps, as key building blocks towards implementation (see figure I.3). However, much attention is often dedicated to the technical development of the single window and the procedures to be handled by the facility, with little attention to the legal implications of the choices made as well as the availability of an enabling legal framework.

As noted earlier much of the technical Single Window development work around the world is focused on the use of ICT, that is, most SW environments anticipate that transactions involving the import, export, and transit of goods that are submitted to and processed by the SW will be done electronically. This reflects, of course, the rapidly growing use of electronic transactions in international trade generally and as part of the development of global supply chains in particular.

There are a variety of technical areas within a SW facility and its cross-border elements in which different technologies can be selected to perform particular functions. For example, an electronic SW system will involve, among other things, the use and creation of electronic documents and data messages, transmission of such documents and messages (which may be done on open networks such as the Internet or in a closed environment such as through virtual private networks), and the retention, storage and archiving of these electronic documents and messages in electronic formats that will enable them to be used in the future for various purposes.

Given the increasing speed and sophistication of ICT development, there is an element of excitement when considering the array of options available to technologists working on SW development. The development of

SW facilities may seem to be limited only by available resources such as funding, or by political will and management capabilities. However, there can be additional, although often less obvious, limitations that are created by the legal environment in which the national SW may operate.

And because these potential legal limitations are not obvious, it is relatively easy to proceed apace with the technical development of the SW almost in a vacuum. In addition, it is possible that several different technology options will produce exactly the same SW experience for its users (e.g., traders seeking to import or export goods). However, the legal implications of each of these technical models may be quite different.

The kinds of decisions made in the development of the SW, i.e., choosing among many technical options that ultimately lead to the SW's overall system architecture, can affect the options available for creating the legal infrastructure needed for a particular Single Window implementation. Similarly, legal requirements in a particular country's legislation and/or regulations can limit the technology options that can be used in developing its Single Window.[17] For example, if a country's legislation mandates that digital signatures using a private key infrastructure (PKI) approach,[18] then the use of alternative technical approaches to electronic or digital signatures will be limited (see Box I.2). It is suggested that SW development programs work simultaneously on both the technical and legal frameworks in addressing issues related to this "intersection" of law and technology.

In this respect, it should be further noted that, as is the case for the transposition of

BOX I.2. Accommodating future technological developments – the Singapore example

Singapore was arguably the first country in the world to implement the UNCITRAL Model Law on Electronic Commerce in the form of the Electronic Transactions Act (ETA) in 1998. The act established the general legal framework for paperless trade by introducing provisions on e-commerce transactions, on the use of electronic applications by government authorities and on the liability of network service providers. The act also set a framework for the use of public key infrastructure (PKI) for digital signatures.

Singapore has been actively monitoring the developments in the field of e-commerce and in 2010, the ETA was repealed and re-enacted in order to take into account recent advancements and to accommodate future developments. The ETA enacted in 2010 largely retains the previous legal scheme for dealing with electronic transactions. However, there are a number of changes which allow for enhanced flexibility to take advantage of technological developments.

Most importantly with regard to the subject of this Guide, Part IV of ETA was amended to be technology neutral. The previous technology-specific provisions based on the use of PKI have been shifted to a more open approach to accommodate other security procedures such as biometrics as can be seen in the comparison of the relevant provisions:

[17] See generally Luddy, W. J., "International Single Window Development", UNCITRAL Colloquium on E-commerce (New York, 2011); Luddy, W. J., "ASEAN Single Window: The Intersection of Law and Technology" (2008).

[18] It should be noted, of course, that while some countries have adopted a technology-specific approach such as PKI in national legislation, this would be inconsistent with the principle of "technology-neutrality." Additionally, fixing a specific technology in national law makes it difficult to adopt new and more effective technologies as they become available.

BOX I.2. (cont.)

ETA 1998

Secure digital signature 20.

When any portion of an electronic record is signed with a digital signature, the digital signature shall be treated as a secure electronic signature with respect to such portion of the record, if -

A. the digital signature was created during the operational period of a valid certificate and is verified by reference to the public key listed in such certificate; and
B. the certificate is considered trustworthy, in that it is an accurate binding of a public key to a person's identity because -
   i). the certificate was issued by a licensed certification authority operating in compliance with the regulations made under section 42 ;
   ii). the certificate was issued by a certification authority outside Singapore recognised for this purpose by the Controller pursuant to regulations made under section 43;
   iii). the certificate was issued by a department or ministry of the Government, an organ of State or a statutory corporation approved by the Minister to act as a certification authority on such conditions as he may by regulations impose or specify; or iv. the parties have expressly agreed between themselves (sender and recipient) to use digital signatures as a security procedure, and the digital signature was properly verified by reference to the sender's public key.

ETA 2010

Secure electronic signature 18.

1). If, through the application of a specified security procedure, or a commercially reasonable security procedure agreed to by the parties involved, it can be verified that an electronic signature was, at the time it was made -
   a). unique to the person using it;
   b). capable of identifying such person;
   c). created in a manner or using a means under the sole control of the person using it; and
   d). linked to the electronic record to which it relates in a manner such that if the record was changed the electronic signature would be invalidated,

such signature shall be treated as a secure electronic signature.

Source:
http://www.ida.gov.sg/Policies%20and%20Regulation/20100630114202.aspx
http://www.ida.gov.sg/News%20and%20Events/20050907163343.aspx?getPagetype=37
ETA 2010: Available at http://statutes.agc.gov.sg/aol/search/display/view.w3p;page=0;query=CompId%3Aa420994e76d6-4b5f-a5b2-6811a6626054;rec=0;resUrl=http%3A%2F%2Fstatutes.agc.gov.sg%2Faol%2Fbrowse%2FtitleResult s.w3p%3Bletter%3DE%3Btype%3DactsAll
ETA 1998: Available at http://statutes.agc.gov.sg/aol/search/display/view.w3p;page=0;query=DocId%3A%22294c715e-89c8-48c4-8e14-58b9ea4f1c29%22%20Status%3Apublished%20Depth%3A0;rec=0#legis

paper-based processes in an electronic environment, different approaches may be possible based on available resources and vision. At a minimum, the electronic single window will aim at reproducing electronically each step of the paper-based process. A more sophisticated approach will aim at a full paperless process implementation, thus maximizing the benefits arising from the use of electronic media. It should be borne in mind that the migration to the electronic world provides an opportunity for fully rethinking

FURTHER READING

"ASEAN Single Window: The Intersection of Law & Technology", by W. Luddy (May 2008). Available at http://dec.usaid.gov/index.cfm?p=search.getCitation&rec_no=152324

"A Roadmap towards Paperless Trade", United Nations Economic Commission for Europe (2006). Available at http://www.unece.org/cefact/publica/ece_trd_371e.pdf

and re-engineering existing processes, so as not to rationalize existing procedures, but rather to implement brand new procedures specifically designed for the new media. While the complete re-engineering of the processes may not always be possible, streamlining of some of the processes can generally be readily considered along with its legal implications, particularly in terms of data sharing among participating government agencies.

C. The Single Window as an E-Government Tool: *Legal Challenges*

The electronic single window facility lies as a core component of the paperless supply chain, which is a broader concept aimed at promoting cross-border trade, and, therefore, economic development and growth. As a result, the successful implementation of the single window facility is necessary for the establishment of the paperless supply chain, and both goals require an enabling legal environment.

In the trade context data and documents may be exchanged between three main actors: business (B), government (G), and consumers (C). Historically, business has driven the expansion of the use of electronic communications on networks first closed, such as electronic data interchange (EDI) and later accessible to the public, such as the Internet. The cross-border supply chain facilitates commercial transactions between private businesses at each end of the chain; however, interaction with governmental offices is required in order to complete the transaction in compliance with regulatory requirements.

A significant part of the transaction with public offices takes place in the context of the electronic single window, which may therefore be classified as a business-to-government (B2G) application. The electronic single window is also, therefore, a component of the e-government system of a country.

The need to ensure seamless exchange of electronic communications between business and government entities in order to made the electronic SW most effective in facilitating trade poses peculiar legal challenges. In this respect, two different approaches have been observed.

On the one hand, in certain jurisdictions, often belonging to common law systems, general principles are provided for all electronic transactions, while a limited set of special rules for exchanges with government entities (or consumers) may be added as needed.

On the other hand, in other jurisdictions, possibly belonging to the civil law tradition, exchanges among commercial operators fall under rules of general and comprehensive application to that sector, while different separate rules are adopted for electronic communications exchanged with government - or consumers. This approach may ask commercial operators to depart from the standards used for private transactions in light of higher requirements for exchanges with public authorities. Commercial operators may, in turn, be hesitant in embracing the investments needed to satisfy those higher requirements, which result in higher compliance costs.

Moreover, the multiplication of applicable legal regimes may also result in lack of clarity in legislation. This is particularly problematic if interaction with electronic commercial documents (i.e., documents used in B2B transactions) is needed, as higher compliance costs due to a different legal regime for B2G transactions may discourage or prevent commercial operators from submitting data contained in those documents. This situation might occur in cases in which authority requires submission of a trade document that is traditionally only a part of the underlying B2B transactions. And while the exchange between trading partners requires one type of system in this example, the submission to the public authority has different and putatively higher costs.

These considerations may explain why examples of successful implementation of an electronic SW have oftentimes featured the legal approach characterized by common rules for the private and the public sector. Although Singapore's original SW was enabled by specific legislation in 1979, it quickly moved towards this broader approach when it enacted its version of the UNCITRAL Model Law on Electronic Commerce. The exchange of electronic communications with public authorities is now enabled by the general legislation on electronic communications in Singapore, i.e. the Electronic Transactions Act, revised in 2010.[19]

Thus, the necessity of enabling B2G interaction highlights the desirability of a uniform regime for electronic communications applicable to all actors involved. In fact, the underlying economic operation (e.g., a contract for sale of goods) at the core of the cross-border movement of goods should ideally be associated with only one set of data, to be used for all related electronic transactions. As the information originates from the business sector, the legislative environment should accommodate as much as possible the needs of that sector. Hence, the adoption of general comprehensive legislation able to fully address the needs of commercial operators, and whose application is extended to the public sector, is desirable. Such approach, aimed at obtaining information directly from electronic commercial documents may ensure more timely submission of data and better data quality, as only one set of data is used for selective distribution among participants.

Besides smoother B2G interaction, the SW may serve other useful purposes related to e-Government. For instance, the automated creation of an electronic audit trail for all transactions allows more accurate monitoring and workflow optimization by customs and other trade control agencies. This may enable, for example, more precise control of revenues (a G2G application), as well as a prompter reply to queries from the public on the status of their submissions (a G2B/G2Citizen application).

FURTHER READING

"Ten years of single window implementation: Lessons learned for the future" by Koh Tat Tsen, J., Global Trade Facilitation Conference, (Geneva 2011).

Available at http://www.unece.org/fileadmin/DAM/trade/Trade_Facilitation_Forum/BkgrdDocs/TenYearsSingleWindow.pdf

"United Nations Convention on the Use of Electronic Communications in International Contracts", UN-CITRAL (2007). Available at http://www.uncitral.org/pdf/english/texts/electcom/05-89450_Ebook.pdf

[19] Singapore Electronic Transactions Act (Singapore Statutes Chapter 88): "Acceptance of electronic filing and issue of documents 25. —(1) Any public agency that, pursuant to any written law — (a) accepts the filing of documents, or obtains information in any form; (b) requires that documents be created or retained; (c) requires documents, records or information to be provided or retained in their original form; (d) issues any permit, license or approval; or (e) requires payment of any fee, charge or other amount by any method and manner of payment, may, notwithstanding anything to the contrary in such written law, carry out that function by means of electronic records or in electronic form. […]"

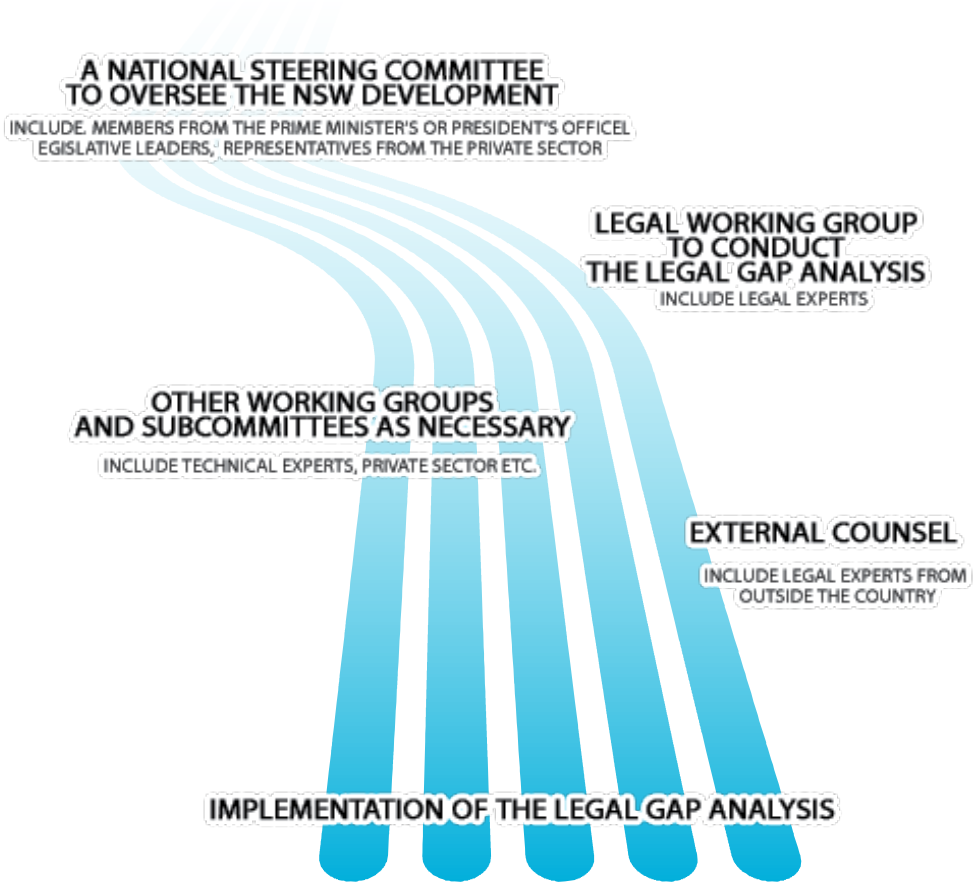
D. Organizational Considerations for Identifying Legal Gaps

Undertaking a legal gap analysis to identify the potential legal barriers for the implementation of an electronic SW is a challenging process and raises a number of important practical considerations. Among these is the institutional or organizational framework in which the work is being done (see figure I.4). For example, some countries have established a national steering committee approach to implementing the SW. The national steering committee should have representatives from the highest level of government. It could include members from the Prime Minister's or President's office, Ministers leading key areas of government that will be involved in the SW, legislative leaders, representatives from the private sector, and so on.

This type of approach helps to insure that the "political will" needed for establishing a SW, which will include input from many different ministries and government departments, is at the centre of the process. The importance of high-level involvement, as well as adopting the necessary legal framework for the SW, is noted as key ingredient for success in UN/CEFACT Recommendation 33, which states:

> *"The most important prerequisites for the successful implementation of a Single Window facility are the political will of the government and the relevant governmental authorities and the full support and participation of the business community. The basic legal framework, including the introduction of privacy laws and rules providing privacy and security in the exchange of information, will also have to be developed."*

Figure I.4. Organizational considerations for the legal gap analysis



Thus, it is important to have a high-level group overseeing the SW development process, particularly since it can help ameliorate any organizational barriers that might hinder SW development. This group will also be key to setting the policy direction for establishing the legal framework for the SW and supporting the underlying legal change, such as new or amended legislation, new decrees or regulatory changes that may be needed based on the gap analysis. Reference may be made to relevant recommendations and guides issued by international bodies when prioritizing and timing actions (e.g., see Box I.3).

In addition, it is helpful to create various "subcommittees" or "working groups" that will be responsible for particular aspects of the SW. Commonly, at least a legal working group and a technical working can be established and would report directly to the national steering committee. These working groups would receive their mandate and terms of reference from the national steering committee. Considering the legal working group, its membership should be comprised of lawyers and legal experts from each of the ministries and/or government departments and agencies that will participate in the SW.

In order to be broad-based from the start of the process, some SW development efforts have included representation from the private sector, either as full participants or as observers. This is not always the case, particularly during the early stages of development, but there can be advantages to involving the private sector at some point in the process to ensure that this key user-group is aware of the benefits of the SW and to build support for this major

BOX I.3. Legal framework development in the WCO single window compendium

Aside from the UNNExT Guide on Single Window Planning and Implementation (available at www.unescap.org/unnext/) developed by UNECE in collaboration with ESCAP, other guides related to SW development also provide guidance on which legal issues should be addressed and when. For example, the *WCO Compendium on How to Build a Single Window Environment* divides the development of a Single Window environment into three distinct phases namely (i) the Incubation & Strategic Planning phase, (ii) Establishment & Consolidation phase and (iii) Development, Implementation, Evaluation & Feedback phase.

During the Incubation & Strategic Planning phase, strategic decisions are taken concerning the nature of the entity that would operate and manage the Single Window environment, services which will be covered and broad directions concerning legal powers of the entity operating the Single Window. In this phase, cabinet decisions or decrees issued by government set the basic ground rules.

In the Establishment & Consolidation phase, the cabinet decisions are translated into action through detailed legislation and/or regulation. During the Establishment & Consolidation phase, the required organizational structures for the Single Window operator and consultative structures to hold discussions with stakeholders covering technical, business process and legal issues are established.

By the time the initiative moves into the development and implementation phase, the basic legal framework should be in place. In any case, it is recommended that before a project proposal with a detailed business case is presented to the government for a decision on the investment, the basic legal framework for operating the Single Window services should already be in place. If during this phase, project evaluation and feedback reveals lacunae, the legal arrangements can be re-visited and corrective measures can be undertaken.

Source: Based on communications with the WCO Secretariat and the WCO compendium available at: http://www.wcoomd.org/files/6.SW_Files/Guidelines_Volumes/PC_SWC_Vol_1_E.pdf

government initiative. For some countries, this would also present an early opportunity for capacity-building in the private sector and assure, as far as possible, early adoption of the SW by supply chain participants and rapid deployment of all aspects of the SW.

Typically, the legal working group (LWG) will be tasked with undertaking the Legal Gap Analysis. While discussed in more detail later in this Chapter, this work would include not only identifying possible gaps in the legal framework for the SW but also the preparation of legal texts (for example, new or amended legislation, decrees, regulations, etc.) that will overcome any legal barriers to implementation of the SW. This work can be done with the assistance of outside counsel depending on the resources, primarily the time of those conducting the gap analysis, available to the LWG.

Unless, however, dedicated and full-time legal resources from within the government can be committed to preparing the legal gap analysis, it may be beneficial to engage outside counsel with specific technology law expertise and experience in the SW and electronic commerce environments to assist and advise the LWG. If outside experts are involved, the LWG will need to prepare the terms of reference for the work and to determine the scope of the work to be done. For example, the scope might be limited to identifying the potential legal gaps in existing law and analysing the alternative approaches for dealing with them. In this case, government lawyers and legal experts may do the actual drafting of new laws, decrees and/or regulations. Alternatively, outside counsel may be engaged in all phases of the legal work assigned to the LWG for developing the legal framework for the SW.

In cases in which the underlying legal concepts for the SW and electronic commerce are relatively new, it may be helpful to utilize legal experts from outside the country to assist in the development of the legal gap analysis. This may be valuable where specialized knowledge of the international legal standards and best practices for implementing a SW is needed to ensure that the SW will be interoperable with other SWs in the development of cross-border trade. Additionally, when engaging outside counsel with this expertise, there may be important opportunities for capacity-building as the LWG works with its members. Technical assistance may also be available from the UN and other international organizations.

As a final comment and while this *Guide* is focused primarily on the development of the legal framework for the SW, countries may have the opportunity to develop their SWs within the context of a regional country or trading group. Here, countries must be attentive not only to the domestic legal infrastructure for their SWs but also to how their SWs will interact from a legal perspective with other States in its region or economic trading group. When participating in such regional developments, the organizational structures that have been developed in some regions may provide useful guidance.

In the ASEAN region,[20] for example, work on the ASEAN Single Window has been developed under the direction of the ASEAN Single Window Steering Committee. The Committee is composed of senior government representatives from each ASEAN Member State and is charged with the responsibility of overseeing the development of both the technical architecture and the legal framework for the ASEAN Single Window. Reporting to and advising the ASEAN Single Window Steering Committee

[20] The Association of Southeast Asian Nations (ASEAN) is composed of 10 member States: Brunei Darussalam; Cambodia; Indonesia; Lao People's Democratic Republic; Malaysia; Myanmar; Philippines; Singapore; Thailand; and Viet Nam. See ASEAN's website at http://www.aseansec.org/18619.htm

are the Working Group on Technical Matters (Technical Working Group) and the Working Group on Legal and Regulatory Matters (Legal Working Group.)

Other organizational formats may also be considered when a country embarks on creating a SW. For countries considering a single window development effort, it may be useful to undertake the exercise of identifying possible gaps in its legal framework prior to the creation of any organizational structure. This may help define the scope of the effort required on the legal side of the Single Window programme and determine what type of organizational structure may be most effective for the development effort itself.

One serious pitfall to be avoided is moving forward with the rapid development of a technical architecture for the SW while not preparing a legal gap analysis and working towards the development of the SW legal framework. This has been seen in various technical development efforts in both the public and private sectors endeavours. It can result in having a SW ready to be implemented technically but not having the framework in place to operate on a legal basis both at the national level and in cross-border transactions.[21] Such a situation can cause frustration on the part of national officials as well as traders whose expectations may have been raised significantly as implementation is delayed, sometimes for significant amounts of time, while the legal barriers to SW operation are eliminated.

The best approach to avoid this scenario is to develop the legal framework for the SW simultaneously or in parallel with the technical development of the SW. This simultaneous work on the legal issues related to the SW will allow the technical design of the SW architecture and its processes to be carried out taking into account the legal requirements. This will be particularly important where the technical architecture for the SW will have major legal implications. Such an approach has been adopted by, e.g., Mongolia (see Box I.4).

BOX I.4. Towards a legal and organizational framework for establishing a single window in Mongolia

Implementing and operating a Single Electronic Window requires an enabling legal environment. To accommodate this need, three laws have been drafted in Mongolia, namely: the E-Signature Act, the E-Transaction Act and the E-Security Act. The Information Communications Technology and Post Authority (ICTPA) and the Legal and International Liaison Working Group have spearheaded the development of legislation to support the national E-government policy.

Mongolia has strived for a coherent approach to E-Governance and consequently an Action Plan was approved in April, 2012. This action plan is expected to help Mongolia to enhance transparency and to expedite provision of electronic services. The implementation of the action plan will last until 2016, and its implementation process and results will be introduced to the Cabinet every first quarter of the year. Within this context, two legislative instruments have already been approved which will support the regulatory framework for the Single Electronic Window: the E-Signature Act, and the Amendment to Civil Law.

The E-Signature Act was approved on 15th of December, 2011. The purpose of the Act is to define the legal basis for usage of electronic and digital signature and to regulate the use of a public key infrastructure within the context of digital signatures. The scope of the act is set in Article 3.1 which states "The issues concerning communications related to the transfer and transmission of electronic documents other than State Confidential Information is governed by this Act." Article 6.3 concerns digital

[21] Particularly in the cross-border context, not having the enabling legal framework in place for national law may raise questions about the "legality" of goods being shipped in international transactions. Risks that might arise, such as delay of cargo release in an importing country or refusing entry of shipments could be of significant concern to traders and might significantly raise the insurance and financing costs for such goods.

BOX I.4. (cont.)

signatures and it provides that "Digital signatures are solely used in order to transfer and transmit electronic documents by government organization and other legal person of state propriety."

In line with the E-Signature Act, amendments were made to Civil Law. In this regard, Article 421.1 states "Paper-based documents, other than transactions to be registered and notarized as stated in the law, are equivalent with documents of electronic form." Parliament resolution No.61 was also adopted. The resolution commits Mongolia to:

1. Systematically develop, plan and implement the transmission of public services provided to citizens into electronic form starting from 1 January 2013.
2. Submit draft legislation to the Great Assembly referring to public services provided to citizens in electronic form.
3. In order to validate the usage of digital signatures to every Mongolian citizens starting from 1 January 2013, develop a smart public key infrastructure with the expense financed from the state budget.

Source: Mongolia Customs (Communication with the UNNExT Secretariat, May 2012)

E. Moving forward: Conducting a Legal Gap Analysis

Identifying the potential gaps in a country's legal infrastructure for implementing the SW requires undertaking research and analysis on domestic laws (legislation, regulations, decrees, judicial decisions, etc.), administrative guidelines and policies, and international agreements. The analysis should cover, in particular, the following matters, many of which are described in more details in Part II of the *Guide:*

1. Electronic transactions legal issues, including:
   a). Legal issues related to identification, authorization and authentication in an electronic transactions environment, including electronic signatures;
   b). Legal requirements for electronic documents and messages;
   c). Need for development of legislation or other regulations dealing with electronic transactions for the SW;
2. Policies (executive acts, instructions circulars, or documents of similar nature), legislative enactments, administrative rulings, regulations and governmental decrees, circulars and the like that would formally establish the SW in national law;
3. Development of a service level arrangement (SLA) for the operation of the SW;
4. Laws and regulations on data protection and information security;
5. Legal and/or regulatory requirements for accessing and sharing information and data between and among government agencies;
6. Legal requirements and regulations on confidentiality and privacy;
7. Laws and regulations relating to data accuracy and integrity for the SW;
8. Liability issues related to operations of the SW, including cross-border transactions;
9. Regulatory/legal requirements for data retention and electronic archiving;

10. Dispute settlement considerations;
11. Intellectual property rights and data base ownership issues, including the ownership of data and information stored or archived in the SW;
12. Examination of banking law for electronic payments in the SW system;
13. Cross-border (mutual) recognition of electronic signatures and, where appropriate, of certification authorities;
14. Legal issues related to conflict of laws in cross-border transactions;
15. The use of electronic evidence, for example, in judicial and enforcement proceedings;
16. Competition law issues (including treaties and conventions, and General Agreement on Tariffs and Trade (GATT)/WTO requirements applicable to the SW);
17. Include an analysis of how international legal standards have been (or have not been) incorporated into a country's legal framework for its SW;
18. Other legal issues that may be identified as important to a particular country's legal regime, for example, laws and regulations for government ministries or agencies, including Customs Administration that will be participating in the SW;

The research should identify and describe, among other things, the main domestic laws, regulations, decrees, legal circulars that arise in the relevant areas of electronic transactions for the SW, related aspects of electronic transactions law, and the legislative and regulatory aspects of a country's customs operations as well as that of other ministries and government agencies related to the import, export and transit of goods. Most importantly, the study should include analysis that identifies any gaps in the domestic legal framework that will need to be addressed for the full implementation of the SW and its cross-border interoperability in an electronic environment.

a. Legal Research Methodology

A methodology and approach typical of a high-level legal research effort is essential for the legal gap analysis (see figure I.5.). Thus, the legal materials included in the research should include:

- **Primary legal sources.** These include, for example, enacted legislation, statutes and laws, decrees, executive orders, circulars, having the force of national law, and formally adopted and promulgated

Figure I.5. Legal gap analysis sources

regulations and rulings, judicial and administrative decisions, among others.

- **Secondary legal sources.** These include, for example, legislative history, ministry, administrative and executive reports that should be reviewed and included to provide background and interpretations of the primary legal materials.
- **References to other legal materials.** Law review articles, conference reports, international commentary, and so on may also be included if relevant to the development of the SW and related electronic commerce legal framework developments in national law as well as cross-border transactions. Particular attention should be paid to uniform legal standards as their international nature may be particularly useful in establishing the legal environment needed for cross-border exchanges. In fact, uniform legal standards may be analyzed as benchmarks in the legal gap analysis.

b. Implementing the Findings of the Legal Gap Analysis

If the development of the SW has begun or a decision has been made to begin development, the legal gap analysis should be explicitly integrated into the overall development timetable and should proceed in parallel with the technical development effort. Once the research is completed, efforts should be commenced to provide solutions immediately. In those cases where national legislation is deemed necessary, the legislative process and timing needs to be considered in the overall objectives for implementing the SW.

Preliminary drafts of proposed legislation should be circulated to legislators and policymakers as soon as possible. Background papers and analysis of the findings of the gap analysis should be included in the legislative package so that all participants will fully understand the policy objectives of the proposed legislation.

Even if the analysis of national law concludes that the SW can be initiated without the adoption of new statutes, efforts should be made to ensure that the regulatory framework satisfies the requirements of an electronic Single Window. This may be the case, for example, where electronic transactions are already authorized in law and the government and its Ministries are in principle allowed to use electronic communications between such Ministries as well as with the private sector.

Some countries have enacted broad electronic transactions statutes that encompass an "e-Government" approach. In at least one case, a government used legislation authorising ministries to use electronic transactions as the legal authority to enable its SW operations and then amended regulations to finetune the use of electronic transactions in its SW.

In addition to legislative actions, it is necessary to assess the need for and use of contractual instruments. For example, it might be necessary to draft and implement interchange agreements to be used between the parties involved in the EDI context (see Box I.5). Detailed and well-crafted agreements on the exchange of electronic data and messages can usefully complement the legislative framework for the SW. Many countries have developed MoUs between their NSWs and participating Ministries. These accomplish the same goals as UN/CEFACT Recommendation 26 but are designed for use between government agencies rather than commercial parties.

BOX I.5. UN/CEFACT Recommendation 26 and interchange agreements for electronic data interchange

In 1995 UN/CEFACT released Recommendation 26 containing model provisions for commercial use of interchange agreements for electronic data interchange. The aim of the recommendation is to promote the use of interchange agreements between commercial parties using EDI within the context of international commercial transactions. The model agreement and its provisions can also be adapted for use within the context of SW facilities.

Interchange agreements are typically made between partners wishing to set the rules for their joint electronic data exchange. Such an agreement details the legal roles and responsibilities of the partners with regard to the EDI operations, including the transmittances, reception and storage of data. Interchange agreements play a significant role when clear governing legal rules and principles are either non-existent or insufficient.

The model interchange agreement incorporated in Recommendation 26 is comprised of several sections including the following:

Section 1. Scope and Structure (including provisions on Scope and reference and applicability of a Technical Annex)

Section 2. Communications and Operations (specifying the standards, security procedures and services, and record storage requirements governing the exchanges of electronic messages between parties)

Section 3. Message Processing (including provisions on when a message is considered to have been received, and rules on electronic message acknowledgement)

Section 4. Validity and Enforceability (including provisions specifying the validity of a transaction made through exchange of electronic messages, the use of the electronic records as evidence, and when a contract is considered formed on the basis of the exchange of electronic transaction)

Other Sections include: ***Section 5.*** Data Content Requirements; ***Section 6.*** Liability; and ***Section 7.*** General Provisions.

The complete model agreement can be found at: http://www.unece.org/fileadmin/DAM/cefact/recommendations/rec26/rec26_1995_r1133rev1.pdf

Part 2:

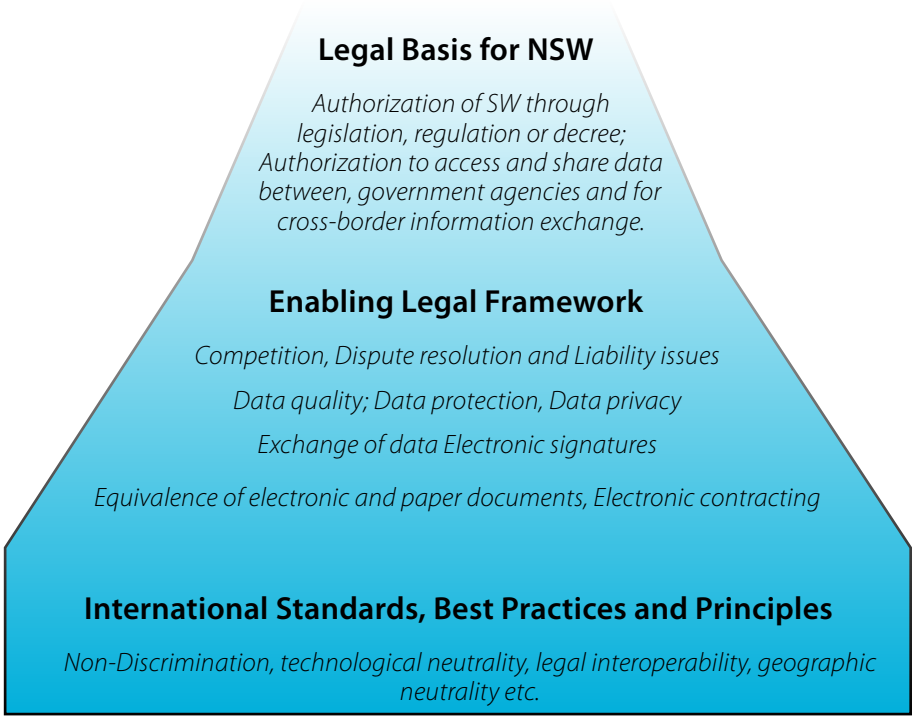
Essential Legal Elements for the Implementation of a National Single Window

A. Single Window Legal Framework Issues

The legal framework underlying the operation of SWs is a mixture of enabling e-commerce and e-transactions legislation and of SW-specific legislation or regulations (see figure II.1). When moving from the general enabling to the more concrete legal basis, the borders are rather vague and the contents of the various pieces of legislation often are arranged as gradients. Typically, the enabling framework consists of a body of legislation which caters to the various needs of the paperless trade environment in general and thus it provides for general rules on, e.g., data privacy and the use of electronic signatures. Those provisions of general application should be based on best practices and internationally accepted standards and principles.

The law in most countries requires some type of legally enabling framework on the part of the government in order for a SW to be established and to operate, especially if electronic. This is particularly important in a cross-border environment where a transaction initiated in one country's SW, where that SW has not been legally enabled, may not be legal in an importing country. For example, some Customs Authorities (or other government agencies)may reject electronic documents from those countries that do not have SW enabling laws that authorize the use of electronic documents and data messaging. Similarly, private sector trading partners may be hesitant about dealing with electronic filings in countries that do not have enabling laws because of the legal uncertainty about such transactions.

Figure II.1. Elements of the legal framework for electronic single windows



Enabling laws for the SW may take the form of legislation, regulations, and/or decrees, depending on the type of legal system in a particular country. And since the fundamental legal principles for operating an electronic SW should be found in general electronic commerce legislation, the existence and content of that general legislation must also be addressed. Developing the SW legal framework includes addressing the following basic issues:

1. National law should authorize SW implementation.
2. National law should authorize electronic commerce transactions.
3. National law should authorize acceptance of electronic documents, records, andmessages in lieu of paper documents/ records/messages in the administrative and judicial systems, that is, national law should implement the international principles of "functional equivalence" and "non-discrimination"

Authorizing the SW can be undertaken in a number of ways. For example, the SW could be created in national law by adopting new legislation or through government Decrees.[22] Alternatively, it may be possible to amend the existing customs law to include authorizing the operation of the SW. In either case it is important to review existing laws that may be affected by implementation of the SW.

For example, various government agencies involved in the import/export process, such as those responsible for sanitary and phytosanitary concerns, may have laws or regulations that could inhibit their full participation in the electronic SW. That is, they may not be authorized to receive or send electronic data messages since law or regulations applicable to them require paper documents and forms only. This barrier to the operation of the SW could be eliminated where a country enacts a broad enabling electronic transactions law that recognizes the functional equivalence of paper documents and electronic communications.

As noted earlier, it is important that whether new law is created or the existing customs law, and/or other relevant law or regulations, are amended for authorizing the legal structure of the SW, a country's approach to its e-Commerce law should be harmonized. That is, as noted earlier, there should not be one legal approach for electronic transactions generally and a different legal approach for the electronic Single Window. This type of legal harmonization can provide a robust legal infrastructure within which all ICT and e-Commerce functionalities can exist. This will be important to traders and other businesses in the private sector since they will not have multiple (and perhaps inconsistent) legal requirements for different parts of their business operations and supply chains.

And finally, national law should make it clear that electronic documents and data messages should be recognized in judicial or administrative proceedings related to a SW transaction. The principle of *non-discrimination* in this regard suggests that an electronic document should not be denied validity solely because it is electronic.[23] This does not mean that all electronic documents must be accepted as evidence in a particular proceeding but only that they should not be rejected solely because of their electronic rather than paper character.

Developing the SW legal framework may involve authorizing the national SW to engage in sharing electronic transmission and acceptance of customs/trade data among and between government agencies involved, as well as across borders with other countries.[24] The latter point is important, as it is now widely recognized that the benefits from national SW and related paperless trade systems would be greatly enhanced if the electronic documents

[22] For example, Lao PDR is in the process of drafting a Prime Minister's Decree that will enable its National Single Window in national law. Similarly, an Executive Order enabled the Philippines National Single Window.

[23] See, e.g., UN Convention on the Use of Electronic Communications in International Contracts, Article 8. Legal recognition of electronic communications; UNCITRAL Model Law on Electronic Commerce, Article 5. Legal recognition of data messages.

[24] Some of the 178 countries that have ratified the 1954 *Convention Establishing a Customs Cooperation Council* have used it as the basis in national law for authorizing the electronic exchange of customs data with other countries' Customs Administrations. This will depend, of course, on how a particular country interprets and implements international treaties, which it has ratified.

generated by them could be used across borders.[25] National SW and other paperless trade providers have already developed membership-based private mechanisms to facilitate exchange of trade-related electronic documents across borders by, in essence, augmenting the existing legislative framework through contract law. However, addressing the issue of cross-border electronic transactions as part the basic SW legal framework development is needed to ensure inclusive participation of all stakeholders and ensure that trade facilitation gains from SW implementation are maximized (see Box II.1).

BOX II.1. Cross-border electronic exchange of trade data and documents: the Pan Asian e-Commerce Alliance (PAA) approach and legal limitations

A number of private sector organizations have also sought to address issues related to the use of electronic signatures in a cross-border context. Among the most prominent are the Bolero System (http://www.bolero.net/en/home.aspx), Electronic Shipping Solutions (http://www.essdocs.com/) and the Pan Asian e-Commerce Alliance (PAA) –http://www.paa.net/PaaPortal/PaaContent/index.htm. The following note focuses on the PAA as it has its roots in the Asia-Pacific region and its membership consists essentially of national single window operators in the region.

PAA is a private sector organization that was founded in July 2000 by CrimsonLogic (Singapore), TRADE-VAN Information Services Co. (Taiwan, Republic of China), and Tradelink Electronic Commerce Limited (Hong Kong SAR). The PAA is the first regional e-Commerce alliance in Asia and it aims to promote and provide secure, trusted, reliable and value-adding IT infrastructure and facilities to enhance seamless trade globally. Combined membership of the parties now exceeds 150,000 organizations, representing almost all active trading enterprises in the Asian market.

In its efforts to enable secure and reliable transmission of trade and logistics documents, the PAA provides the mutual recognition of digital certificates issued by members' Certificate Authorities for use in electronic documents exchanged among the parties who have entered into the PAA agreements, and allows inter-connection of network services to provide e-Commerce transaction application services for the business community.

With the PAA cross-border transaction service, exchange of such documents may be conducted electronically across borders over a secure PAA infrastructure and with ease and efficiency. In addition, users will be able to re-use the relevant data from the received documents for the application and submission of trade or regulatory declarations with the local regulatory bodies in those economies in which PAA members operate.

A PAA Certificate Authority has been commissioned as a private framework for the mutual recognition of PKI. An infrastructure to support both end-to-end digital signatures as well as digital signatures between service providers has been established. The alliance is targeting to have at least one Certificate Authority from each member country to be certified and participate in the PAA.

A cargo tracking service will be incorporated into the cross-border transaction servicesto provide information to freight forwarders on the status of their cargo.

PAA provides a set of legal agreements, specification and procedures that privately enforces the legality of the electronic transactions within the PAA network through contract law. Within this network, the import and export trade declarations, electronic cargo manifest, electronic shipping orders, etc. in the e-commerce of trade may operate smoothly.

[25] See, e.g., ESCAP Resolution 68/3 on "Enabling paperless trade and the cross-border recognition of electronic data and documents for inclusive and sustainable intraregional trade facilitation" (2012).

BOX II.1. (cont.)

On the other hand, the lack of a common regulatory framework for international electronic transactions is deterring trading entities from carrying out cross border business dealing. PAA has multiple limits in its operation. Firstly, PAA rules and norms are merely operable within its network, rather than in the whole Asia-Pacific region. Secondly, PAA rules and norms are, by nature, private contracts among their members, and not national or international law.

In international trade, contractual arrangements can, in most circumstances, pre-empt the application of non-mandatory legal norms and as long as there is no dispute between trading partners, define their rights and obligations. However, contractual arrangements still need to comply with domestic national laws of mandatory application and when disputes are cross-border, relevant international law provisions. This compliance is critical to ensure the recognition and enforcement of judgments and arbitral awards rendered on the basis of contractual agreements. This will be particularly true where there are disputes arising from the contracts and the parties have to rely on the "external" interpretations or enforcement of their contractual arrangement. Further, where disputes involve third-parties, i.e., individuals or entities that are not a party to PAA contract agreements, those third parties may not seek resolution under the PAA rules and norms.

Although traders' initiatives based on contractual agreements, such as those of the PAA, should be encouraged, they complement, but do not substitute a treaty-based legal environment, which offers a higher level of legal predictability due to its mandatory nature and applicability. Such treaty-based environment may include a Regional Agreement to ensure the safe and secure exchange of trade data and documents in cross-border trade in the Asia-Pacific region as well as enabling texts at the global level such as the UN Convention on the Use of Electronic Communications in International Contracts.

Source: Based on Xue, Hong, "Note on the legal limitations of the PAA approach" (April 2012).

FURTHER READING

"Model Law on Electronic Commerce with Guide to Enactment", UNCITRAL

Available at: http://www.uncitral.org/pdf/english/texts/electcom/05-89450_Ebook.pdf

B. Authenticity and Integrity: Electronic Signatures

a. Electronic Signatures – A General Introduction.

The use of *electronic signatures* [26] (including digital signatures), which may involve certification authorities, are aspects of the legal infrastructure that should be considered when creating the enabling legal environment of the SW. Mutual recognition of certification authorities (who certify certain digital signatures) can be important as well in cross-border transactions and are discussed in this section of the *Guide* as well.

An electronic signature is the broad term that encompasses various types of "signatures" in electronic formats and the methods used to create them. An important purpose of these types of signatures is to provide the equivalent to handwritten signatures and other types of devices (for example, seals and rubber signature stamps) used in the paper

[26] See, UNCITRAL Secretariat (2009), Promoting Confidence in Electronic Commerce: Legal Issues on International Use of Electronic Authentication and Signature Methods (2009). This guidance document, taken as a whole, provides a broad and very useful discussion of most of the relevant electronic signature methodologies as well as the important legal considerations associated with each.

environment. In its 2009 guidance document, the UNCITRAL Secretariat defines several broad categories of electronic signatures and authentication methods. Below are the major types:

- Electronic signatures based on the knowledge of the user or the recipient, for example, a person knowing certain passwords or personal identification numbers (PINs). These might include clickable "OK" or "I confirm" boxes used on secure websites where the user has already logged in using a password or PIN;
- Electronic signatures based on the physical features of the user, for example, biometrics such as an individual's handwritten signature using a digital pen on a digitizing pad;
- Electronic signatures based on the possession of an object (sometimes called a "token") by the user, for example, the codes or other information stored on a magnetic card; and,
- Other types of authentication and signature methods that might be used to indicate the originator of an electronic communication include a facsimile of a handwritten signature or a name typed at the bottom of an electronic message or email.[27]
- Higher levels of security may be obtained by combining the methods above, e.g., by requiring the use of an authenticating factor related to knowledge, and of another authenticating factor related to possession.

The type of electronic signature required in a particular situation should be based on the level of security that is needed for that particular transaction. Not all transactions require the highest level of security (which may carry with it very high costs relative to a particular transaction). "Digital signatures" are a subset of electronic signatures and *digital signature* is usually the name given to technological applications that use

BOX II.2. On Public Key Infrastructure (PKI) systems

PKI systems generally involve the use of two "keys." One key is private and only the sender of the message or document knows it; the other is a public key, which is provided to the recipient(s) of digitally electronic messages or documents. A complex mathematical formula or prime number algorithm based on the private key creates the public key. Thus, the two keys are "associated" or complement each other. The sender digitally signs the message or document using the private key and if the sender's public key matches the digital signature, the receiver can be reliably certain that the message is from the person claiming to be the sender.

But a private key and a public key are simply a pair of two numbers and are not automatically associated with any particular person. Thus, there may need to be some way of associating the keys with a particular sender or to verify that the digitally signed message or document is indeed from the person with which it claims to be associated. Certification Authorities (CA), also called *certification service providers*, as in the UNCITRAL Model Law on Electronic Signatures,[28] add value in PKI systems by providing the linkage between the two keys.

A CA can issue a "certificate" (an electronic record) that shows the public key and the name of the certificate subscriber as the subject of the certificate and, usually, confirms that the subscriber is the owner of the private key associated with the public key. The primary purpose of the certificate is to bind the public key with a particular signatory. This enables the recipient to further verify that the signature is valid and that some portion of the data message has not been changed or modified since it was digitally signed.

[27] See UNCITRAL Secretariat (2009), para. 16.

[28] UNCITRAL Model Law on Electronic Signatures, art. 2(e): "Certification service provider" means a person that issues certificates and may provide other services related to electronic signatures.

asymmetric cryptography, for example, PKI approaches which are elaborated upon in further detail in Box II.2.

In the cross-border or international trade environment, there may be a need to determine whether a certification authority (CA) in a different country is authorized to provide a valid certificate for a particular electronic signature. While a party may know the CAs in his own country, the question may arise as to how to "trust" the certificate issued by a CA outside the country since it may not know, for example, what standards are used to establish CAs in that country. This is the subject matter of issue of "mutual recognition".[29]

One approach that has been adopted in a few countries that have requirements for digital signatures with certificates has been not to accept foreign CA certificates unless that CA has an office in the receiving country and has been accredited by the domestic national authority. This is considered by some to be a less than trade-friendly approach and can increase the costs of cross-border trade. It can also result in trading partner countries placing similar requirements for CA from those countries. Finally, countries may wish to consider whether creating this type of requirement could be considered a trade barrier that might violate a country's obligations under free trade agreements or its obligations under WTO agreements.

One solution, though not necessarily the only one, that has emerged is the use of ***mutual recognition agreements*** (MRAs) between countries, usually in a PKI environment. Under this type of agreement, the CA certificates (or designated CAs) from one country are accepted by the other. That is, they have reciprocity under the MRA. Often, the terms of an MRA describes the standards that CAs must meet in each country and require that that each country's appropriate authority audit designated CAs on a regular basis.

Another approach adopted by some countries is simply to recognize in their law that an electronic signature from a foreign CA will be accepted if it has the same level of reliability as one provided domestically. The definition of electronic signature includes, obviously, digital signatures based on PKI and related certificates.

For any country's SW development work, the choice of the particular type of electronic signature or signature system will depend on a variety of factors. These include national policy decisions about the use of electronic signatures in electronic commerce generally as well as the desired level of security for and risks associated with transactions in its SW. A further consideration may be the costs associated with implementing various electronic signature methods. But where a high level of security is needed, or where the risks associated with particular transactions are high, an electronic SW may wish to consider a higher level of electronic signature and establish appropriate requirements in its regulations accordingly.

In this respect, it should be noted that policy decisions underlying e-customs/e-Government applications may consider requiring higher security standards, often currently achieved by adopting PKI technology.[30] At the same time, purely commercial transactions adopt more flexible standards based on actual needs. Thus, while e-banking transactions may use applications of PKI technologies, other purely commercial electronic exchanges may rely on simpler technologies. If data from purely commercial exchanges needs to be input in the SW, it is critical to design entry points for input from those sources while preserving the system's overall security. As a matter of overall national policy, of course, a country may wish to maintain flexibility in the requirements it establishes for electronic signatures generally, particularly in light of the principle of "technology neutrality".

[29] See also Box II.2

[30] However, some major international trading countries such as the United States of America use a simple ID/Password approach to permitting access to its SW.

Whatever requirements may be set for a particular SW environment,[31] however, care should be taken to ensure that they do not prevent the adoption of newer and more innovative technologies as they emerge. For example, it may be possible to include in national law a flexible standard regarding electronic signatures, and thus permit the use of any type of electronic signature appropriate for a particular transaction. This would be consistent with the international legal standard set out in the UNCITRAL Model Laws as updated by the United Nations Convention on the Use of Electronic Communications in International Contracts. At the same time, government organizations with special needs in this area may be authorized to develop, perhaps in collaboration with a central authority, requirements for electronic signatures that can be implemented through its SW regulations.

b. Identification, Authentication, and Authorization

Access to the SW, whether by private sector traders or government ministry staff, should be controlled and appropriate regulations should be adopted to achieve this result. This is important for many reasons including data protection, quality and accuracy, data integrity, and information security within the SW. The ability to properly identify, authenticate, and authorize those who will have access to the SW requires appropriate regulatory procedures.

Common definitions of "identification", "authentication" and "authorization" in the SW environment include:

Identification: This is the ability to reliably and consistently identify entities seeking access to the SW such as traders or personnel from various government ministries or agencies who may need to obtain information from, or provide information to, the SW. For example, a simple "user ID" could be assigned to each individual who is permitted to access the SW. Identification may require the presentation of "off-line" credentials released by a particularly trusted third party (e.g., paper-based national ID).

Authentication: After establishing a method for identifying a particular user, it is important to determine that the identity presented is assigned to the person who is using it. The most common way to determine that the person who has entered a "user ID" is for that person to enter a "password" that is known only to that person and the "system" into which it is entered. This is the process of authentication or of indentification verification. Thus, when someone tries to log onto the SW system using a particular user id, the entry of the correct password will grant access to the SW. Put differently, the user ID uniquely identifies the user to the system and the password can be used to verify or authenticate the identity of the user attempting to log onto the SW. Authentication may be performed by the system to which access is requested, or by a trusted third party.

Another example involves the use of a bankcard to withdraw funds from a personal bank account. First, the account holder inserts the card into the bank machine. The card is a "token" that provides the "identity" of the person seeking to withdraw the funds. But how does the bank know that the person in possession of the card is really the owner, that is, how can the bank "authenticate" the person's identity? Again, the most common way to do this is for the individual to enter a PIN that only the individual and the bank know.

Authorization: This is the act of granting permission for someone or something to conduct an action in the SW environment. Even when the identity and authentication process has indicated who someone is, authorization may be needed to establish what he or she is allowed to do. In the SW, for example, some individuals may be authorized to input data to the SW but not to view or change other data that may be held in the SW.

[31] It should be noted that although a SW environment may chose a particular technology, a country may wish to avoid adopting a narrow standard in national law.

In the course of establishing the regulations for operation of an electronic SW, therefore, it is important to provide for the process of identification, authentication and authorization for each class of individuals who will be permitted to access the SW. For example, different classes of individuals might include, private sector traders/brokers, employees of customs, employees of other government organizations, enforcement authorities, etc. Certain particularly qualified operators (for example, "Authorised Economic Operators"[32] under an established programme with Customs) may qualify, in light of the frequency and value of their interactions with the SW, for closer system integration, for receiving customized software allowing for a higher level of interaction with the SW. Such process should not however unduly penalize other operators.

In a regional or multi-country SW grouping, participants will likely look at how the SW in each participating country has established such regulations and procedures in order to feel assured that access to a SW is controlled for information and data security as well as other related reasons noted above. One approach to simplify this process would be for the regional country group to establish a standard or harmonized set of requirements that each participating member-country agrees to implement.

C. A Broader Single Window and Electronic Signature Perspective

The materials in this Section of the *Guide* provide a deeper exploration of some of the key legal issues related to the use of electronic signatures by both the private and public sectors as related to the SW environment and trade in general. It is designed to provide specific legal guidance to policymakers who will make overarching decisions regarding the choice of electronic signature approaches that can be implemented in the national legislative framework for electronic commerce and for the implementation of the SW.

a. Preliminary Considerations

One of the most common questions raised in the context of developing an electronic SW is what type of electronic signature approach should be adopted. Sometimes the parties exchanging the communications are already acquainted, but in other cases they are not. In any case, there is the need to ensure that the parties in the real world correspond to the entities that they purport to be in the electronic world, and that the communications exchanged are indeed those meant to be sent by their originator, including with respect to communicating adequately the significance attached to them by the author. Such issues are usually referred to as matters of authenticity and integrity of the data message, and they are often dealt with in the context of the use of electronic signatures. And these general factors apply equally in B2B and B2G transactions related to the SW.

In fact, the reference to the notion of "signature", developed for paper-based instruments, may be misleading. Traditional signatures may fulfill a number of different functions, and provide varying levels of reliability. For instance, some signatures may identify the author of a document, or express the consent to be bound by a document; in other cases, the identification of the signatory may be reinforced by the intervention of a third party at the moment of the signature, such as a notary public. In other, rarer cases, signed documents may also contain third-party information on the time and date of the signature, and on the integrity of the documents.

Electronic signatures may provide accurate information on the origin and integrity of the document, if adequately designed. At the same time, excessive requirements with respect to the technology required for electronic signatures, although deemed useful to ensure maximum certainty, may actually hinder the wider use of electronic signatures by imposing on users excessive

[32] See e.g., WCO Compendium of Authorized Economic Operator AEO Programmes (July 2010). The AEO approach is an important component of the WCO Framework of Standards to Secure and Facilitate Global Trade (SAFE) and was adopted by the WCO members in 2005. Further information about the Safe Framework can be accessed at http://www.wcoomd.org/home_pfoverviewboxes_safepackage.htm

costs. Therefore, well-designed information systems, including electronic SW facilities, should strike a balance between certainty and flexibility, based on an assessment of the needs of different categories of users as well as considerations related to the costs of this aspect of the system.

Another important element to be considered when choosing the appropriate type of electronic signature is the fact that trust may not depend only on technology. A number of other elements may be relevant to establish a trusted relation, such as previous exchanges, or inperson interaction. The quantity and value of the communications exchanged may also be relevant: occasional communications of small value could rely on less demanding technological requirements than those requested to validate a regular flow of information submitted by a major trading company or a single very high value transaction.[33]

In the SW environment, the issue demands additional considerations. First, the SW facility may be conceived as a closed system, requiring identification of users before releasing the credentials necessary to access the system.[34] However, such approach could also pose an obstacle to the interaction with private business, especially small and medium-sized enterprises and commercial operators in countries with limited ICT access, thus preventing the submission of commercial documents to the SW. In general, the need to cater to the ever increasing openness of information systems should be borne in mind, as well as technological limitations that may arise from the growing need to use mobile devices for data input.

b. Legislative Approaches to Electronic Signatures

It is possible to group legislation dealing with electronic signatures under three main approaches (see figure II.2): (a) the minimalist approach; (b) the prescriptive (or technologyspecific) approach; and (c) the two-tiered or two-pronged approach.

Figure II.2. Elements of the legal framework for electronic single windows

The Minimalist Approach	*The Two-Tiered Approach*	*The Prescriptive Approach*
All Technologies for electronic signature are recognized on an equal basis if the technology satisfies certain requirement	In general, all electronic Signature methods are recognized as potentially having legal value but certain technologies offering higher levels of security are associated with a stronger legal status	Demands the use of a specific technology
Accommodates future developments Avoids rapid obsolescence Allows parties to choose the type of technology appropriate to their needs	Balanced benefits and trade-offs	Offers certainty but poses a number of potential challenges and can hinder the adoption of future technologies
Technology Neutral	**Balanced**	**Technology Specific**

[33] The use of Quantum Key Distribution, considered as one of the most secure encryption technologies currently available, may provide a good example of the factors relevant in the choice of the appropriate technology.

[34] This approach could be preferred on the basis that it is considered a transposition in the electronic world of the role and function of customs brokers.

Under the minimalist approach, all technologies for electronic signature are recognized on an equal basis, provided that the technology employed satisfies the function of the handwritten equivalent by meeting certain requirements, in a strict implementation of the principle of technological neutrality. This model offers two main advantages. Since it is technologically neutral, i.e., it does not rely or refer to any particular type of technology, it is able to accommodate future developments and avoid rapid obsolescence. Moreover, it allows parties to choose the type of technology appropriate to their needs. A common legislative standard for establishing generic functional equivalence between electronic and handwritten signatures is contained in article 7, paragraph 1 of the UNCITRAL Model Law on Electronic Commerce[35] and the more recent formulation contained in Article 9(3) of the UN Convention on the Use of Electronic Communications in International Contracts (ECC).[36]

The prescriptive model demands the use of a specific technology, typically digital signatures, such as signatures based on asymmetric cryptography and PKI, which could also satisfy additional functions, such as a guarantee of the integrity of the electronic message and a timestamping service.[37]

The role of the government in managing PKI systems may vary, as providers of certification services may be required to obtain prior authorization or licensing from a public authority or may be encouraged to join voluntary arrangements. The government may further increase control by establishing an exclusive central authentication service provider. This approach is partly justified by the fact that electronic communications provide possibilities unmatched in the traditional world.

In addition to ensuring the highest level of security, the prescriptive approach offers certainty on the technologies acceptable for electronic signatures. However, it also poses a number of potential challenges, since requirements for electronic signatures may not find an equivalent in the legislative requirements for handwritten ones, thus violating the principle of nondiscrimination of electronic transactions against paper-based ones. Moreover, the mandatory use of certain technologies could hinder the adoption of future ones or may overstate the benefits of those adopted, especially when not yet fully mature. A change in the technology choice may require formal legal amendments that are time and resource-consuming. This model may likely impose additional financial costs on users, thus detracting from the economic benefits associated with the use of electronic means.

In a SW environment, the adoption of a prescriptive approach could result in demanding users to adopt PKI technology, resulting in the use of PKI certificates. This would probably allow users to achieve the level of security needed[38] for sensitive information relating to cross-border trade and customs operations. On the other hand, this could also result in creating obstacles to interaction with users who are not willing or in a position to use those certificates. Therefore, exceptions to the use of PKI technology may need to be foreseen.

[35] Article 7, paragraph 1 of the UNCITRAL Model Law on Electronic Commerce refers to two main functions of handwritten signatures: to identify the signatory and to link the signed information with the signatory.

[36] Article 9(3) of this Convention states: "Where the law requires that a communication or a contract should be signed by a party, or provides consequences for the absence of a signature, that requirement is met in relation to an electronic communication if: (a) A method is used to identify the party and to indicate that party's intention in respect of the information contained in the electronic communication; and (b) The method used is either: (i) As reliable as appropriate for the purpose for which the electronic communication was generated or communicated, in the light of all the circumstances, including any relevant agreement; or (ii) Proven in fact to have fulfilled the functions described in subparagraph (a) above, by itself or together with further evidence.

[37] In reality, the actual use of PKI-based signatures is not as widespread as sometimes predicted. Furthermore, those applications based on encryption techniques which are commonly used and provide significant benefits do not perform functions similar to those related to the traditional notion of signature: see, e.g., J. Winn, "The Emperor´s New Clothes: The Shocking Truth About Digital Signatures and Internet Commerce", 37 *Idaho L. Rev.* 353 (2001), p. 376, citing the example of Secure Sockets Layer technology (SSL, now known as Transport Layer Security – TSL) widely used, for instance, in electronic banking.

[38] It should be noted that it is not the case that PKI necessarily offers a high level of security. The level of security depends on how the PKI is implemented and run, including the identification process and audits. Some have suggested that it provides the basis for "non-repudation" but from a legal perspective this may not be the case.

In more general terms, however, it is necessary to draw a distinction between the formulation of general laws relating to the legal recognition of electronic signatures, and the designation of specific technologies or methods in the implementation of SW systems. This is the distinction between the enactment of enabling laws relating to electronic signatures, and the application of those laws in a specific situation. An enabling approach, of course, is recommended for the former.

Regarding the latter distinction however, it is wholly possible for the implementing agency to specify the use of a particular electronic signature technology or method for the SW system, which all users of the SW system (or sub-system) will have to use. The legal recognition for such electronic signature could be based on laws enacted under a minimalist approach, prescriptive approach, or two-tiered approach, as the case may be, but the generality of any such law should not mean that a SW system would be built in such a way that users can pick and choose any manner of electronic signature technology or method that they might wish to use to interact with the SW system. Whether a SW system can be built in a way that permits the use of different types of electronic signatures in different parts of the SW system, would depend on an analysis of the need, cost-effectiveness and practicality of such a design.

Thus, a balance between security and flexibility may be achieved under the "two-tiered" or "two-pronged" approach. This model foresees two levels of requirements for attributing legal validity to electronic signatures. In general, all electronic signature methods are recognized as potentially having legal value, to be ascertained in case of dispute in light of factual circumstances and other relevant factors, including the parties' contractual agreements.

Moreover, certain technologies offering higher levels of security are associated with a stronger legal status, for instance, by reversing the burden of proof on the origin and integrity of the message, provided certain requirements are met. Those requirements may be described in technologically neutral terms or may refer to specific technologies; they may also go as far as demanding specific certification models, so that, for instance, only certain certification service providers would qualify to offer electronic signatures for specific applications.[39]

It is important to note that the rules relevant for electronic signatures may be found in several different legal sources, which include: treaties and conventions; model laws; regional and national legislation (often based on the UNCITRAL model laws); self-regulatory instruments such as codes of conducts; and contractual agreements. Naturally, treaties, conventions and models are relevant if they have been incorporated into and form a part of national law.

Box II.3 is a short description of the legislative approach taken by Singapore, where the legislator has taken steps to create an extensive body of enabling legislation with regard to the use of electronic signatures.

BOX II.3. On the Singaporean legislative approach to electronic signatures

The legal framework underpinning Singapore's national SW addresses data authenticity issues in its Electronic Transactions Act (ETA). The ETA stipulates on electronic signatures as follows:

Section 8 – Requirement for signature.

Where a rule of law requires a signature, or provides for certain consequences if a document or a record is not signed, that requirement is satisfied in relation to an electronic record if —

a. a method is used to identify the person and to indicate that person's intention in respect of the information contained in the electronic record; and

[39] The Electronic Transactions Act of Singapore of 1998 is an early example of legislative enactment of the twotiered approach. Article 6 of the UNCITRAL Model Law on Electronic Signatures of 2001 may also be regarded as providing a blueprint for this model.

BOX II.3. (cont.)

b. the method used is either —
   i). as reliable as appropriate for the purpose for which the electronic record was generated or communicated, in the light of all the circumstances, including any relevant agreement; or
   ii). proven in fact to have fulfilled the functions described in paragraph (a), by itself or together with further evidence.

Section 17 – Secure electronic record.

1. If a specified security procedure, or a commercially reasonable security procedure agreed to by the parties involved, has been properly applied to an electronic record to verify that the electronic record has not been altered since a specific point in time, such record shall be treated as a secure electronic record from such specific point in time to the time of verification.

2. For the purposes of this section and section 18, whether a security procedure is commercially reasonable shall be determined having regard to the purposes of the procedure and the commercial circumstances at the time the procedure was used, including —

a. the nature of the transaction;
b. the sophistication of the parties;
c. the volume of similar transactions engaged in by either or all parties;
d. the availability of alternatives offered to but rejected by any party;
e. the cost of alternative procedures; and
f. the procedures in general use for similar types of transactions.

Section 18 – Secure electronic signature.

1. If, through the application of a specified security procedure, or a commercially reasonable security procedure agreed to by the parties involved, it can be verified that an electronic signature was, at the time it was made —

a. unique to the person using it;
b. capable of identifying such person;
c. created in a manner or using a means under the sole control of the person using it; and
d. linked to the electronic record to which it relates in a manner such that if the record was
e. changed the electronic signature would be invalidated,
f. such signature shall be treated as a secure electronic signature.

2. Whether a security procedure is commercially reasonable shall be determined in accordance with section 17(2).

Third Schedule to the ETA

Secure electronic record with digital signature

2. The portion of an electronic record that is signed with a digital signature shall be treated as a secure electronic record if the digital signature is a secure electronic signature by virtue of paragraph 3.

Digital signature treated as secure electronic signature

BOX II.3. (cont.)

3. When any portion of an electronic record is signed with a digital signature, the digital signature shall be treated as a secure electronic signature with respect to such portion of the record, if —

a. the digital signature was created during the operational period of a valid certificate and is verified by reference to the public key listed in such certificate; and
b. the certificate is considered trustworthy, in that it is an accurate binding of a public key to a person's identity because —
   i). the certificate was issued by an accredited certification authority operating in compliance with the regulations made under section 22;
   ii). the certificate was issued by a recognised certification authority;
   iii). the certificate was issued by a public agency approved by the Minister to act as a certification authority on such conditions as he may by regulations impose or specify; or
   iv). the parties have expressly agreed between themselves (sender and recipient) to use digital signatures as a security procedure, and the digital signature was properly verified by reference to the sender's public key.

The ETA also establishes a voluntary licensing regime with the relevant licensing criteria for Certification Authorities and designates the Controller of Certification Authorities.

Source: Electronic Transactions Act, Singapore.
Info-communications Development Authority of Singapore
http://www.ida.gov.sg/Policies%20and%20Regulation/20060526123350.aspx

c. Legislative Models for Electronic Signatures

In line with general principles, and in order to facilitate interaction between the single window and commercial operators, it is recommended that electronic signature requirements for the SW should be same as those adopted in general legislation. It is desirable to have a flexible approach that can provide higher levels of security to critical applications when appropriate but also accommodate inputs from less sophisticated users when possible.

In practice, a limited number of legislative models are available.

On the one hand, UNCITRAL texts, and, in particular, the UNCITRAL Model Law on Electronic Signatures of 2001 and the UN Electronic Communications Convention of 2005 may provide a useful blueprint for the legislator. The ECC, as noted earlier, provides in article 9 the most modern UNCITRAL formulation for a rule on electronic signatures.

On the other hand, the European Union directive on electronic signatures is another text exercising significant influence also beyond the region of origin.[40] However, this text has been implemented in different manners in European Union Member States themselves. Since the directive defines more precisely the legal status of signatures offering a higher level of reliability,[41] the directive has been alternatively understood as based on a "two-tier" or on a "prescriptive" approach.

[40] Directive 1999/93/EC of the European Parliament and of the Council of 13 December 1999 on a Community framework for electronic signatures, Official Journal of the European Communities, L 13, 19 January 2000.

[41] The directive identifies three different forms of electronic signatures, i.e. the "simple electronic signature", the "advanced electronic signature" (AES) and the "qualified electronic signature" (QES): Commission of the European Communities, Action Plan on e-signatures and e-identification to facilitate the provision of crossborder public services in the Single Market, COM(2008) 798, 28 November 2008, p. 6. In practice, this classification points at increasing levels of authentication. Thus, while the legal conditions for the "simple electronic signature" could be met by the use of any technology, the requirements for the "advanced electronic signature" could be fulfilled by the use of a digital signature based on PKI, and those for the "qualified electronic signature" by the use of a digital signature based on PKI and of a smart card.

The European Union directive was successful in promoting the use of electronic signatures in European Union Member States by giving them a more certain legal status.[42] However, due to those differences in national implementation, the directive is currently under review.[43] Future work of the European Union seems directed towards improving cross-border interoperability of advanced and qualified signatures, including by building on identity management systems developed for use in transactions with public entities (see Box II.4).[44] Generally, it should be born in mind that developments in the field of identity management (IdM) may have a significant impact also on the law of electronic signatures.

BOX II.4. Revision of the eSignature directive in the European Union

Under the Digital Single Market Pillar of its Digital Agenda, the European Commission has developed a revision of the eSignature Directive with a view to provide a legal framework for cross-border recognition and interoperability of secure eAuthentication systems.

Electronic identity (eID) technologies and authentication services are essential for all kinds of online transactions. Today, log-in usernames and passwords are among the most common online authentication systems. While these systems are adequate for many applications, more secure solutions are increasingly needed to protect personal data online.

Creating eID systems that work at the European level is an important part of building a safe and secure zone spanning all countries of the European Union. Developing an acceptable system requires close cooperation between Member States as well as wide-ranging consultations of both direct stakeholders and the general public across Europe.

What has the European Commission done? In 2010-11, it set up a formal expert group to assist the Commission in drafting the revised directive. It then consulted Member States and industry on issues related to eID, prepared a Commission Communication on eID, authentication and signature policy, and further consulted stakeholders and prepared an impact assessment for the revised Directive with a view to give permission to the European standards organizations to develop eID standards that could be used across the EU.

In June 2012, the proposal for a Regulation "on electronic identification and trusted services for electronic transactions in the internal market" was adopted by the Commission. The new framework for electronic identification and electronic trust services will:

1. Ensure mutual recognition and acceptance of electronic identification across borders;
2. Give legal effect and mutual recognition to trust services including enhancing current rules on e-signatures and providing a legal framework for electronic seals, time stamping, electronic document acceptability, electronic delivery and website authentication.

This proposal represents the first milestone in the implementation of the objectives of the Legislation Team (eIDAS) Task Force set up by the Commission in order to deliver a predictable regulatory environment for electronic identification and trust services for electronic transactions in the internal market to boost the user convenience, trust and confidence in the digital world.

Source: European Commission http://ec.europa.eu/information_society/newsroom/cf/fichedae.cfm?action_id=167&pillar_id=43&action=Action%208%3A%20Revision%20of%20the%20eSignature%20directive and http://ec.europa.eu/information_society/policy/esignature/eu_legislation/regulation/index_en.htm

[42] Commission of the European Communities, Report on the operation of Directive 1999/93/EC on a Community framework for electronic signatures, COM(2006) 120, 15 March 2006, p. 9. para. 5.1.
[43] European Commission, Digital Agenda for Europe, Action 8: Revision of the eSignature directive: http://ec.europa.eu/information_society/newsroom/cf/fichedae.cfm?action_id=167&pillar_id=43&action=Action%208%3A%20Revision%20of%20the%20eSignature%20 directive
[44] Commission of the European Communities, Action Plan on e-signatures and e-identification, cit.

d. Cross-border Recognition of Electronic Signatures

Peculiar challenges are posed by the cross-border recognition of electronic signatures, a goal that has, so far, proven to be largely elusive and that is perceived as a major obstacle to the broader use of electronic documents in cross-border trade.[45] The issue is relevant in the design and operation of cross-border SW facilities to the extent that its design contemplates the receipt of electronic documents and data messages from parties not located in the receiving SW State.

The size of the problem of cross-border recognition of electronic signatures would depend, of course, on the design and extent of the cross-border linkages between SWs and what purpose the foreign document or data are intended to fulfill. For example, there may be legal and practical difficulties associated with the use of foreign electronic evidence in the enforcement of the customs or other regulatory laws.

Some Customs Administrations and other regulatory agencies may want the declarant (i.e., a person or entity submitting the declaration) to be a person (e.g., an agent) within jurisdiction (and not situated outside jurisdiction.) That person or entity would take responsibility for the accuracy of the contents of the application. Therefore, from the perspective of the importer (or the importer's agent) and the customs or other regulatory agency, the business processes in the SW might not want to require the transmission of documents or data from a foreign third party (e.g., the exporter), as the import declaration and supporting documents should be submitted by the importer (or importer's agent) within jurisdiction, who has to take responsibility for them.

In such a scenario, there would be no necessity for cross-border recognition of electronic signatures, as the electronic signature applied to the import declaration and supporting documents would be that of the importer (or importer's agent) and would be recognised in accordance with conditions imposed by the importing country's authorities.

In order to create efficiencies for the importer, a wider SW electronic network can make it possible for the exporter to share data with the importer, which the importer can re-use in creating and submitting the import declaration. But no cross-border recognition of electronic signature of the exporter would be necessary in such a case, as it is the importer who submits the import declaration (incorporating re-used data) sealed with the importer's electronic signature. As noted earlier, the choice of technical design of a SW will impact on the type of legal issues raised (or avoided), and in this case, the choice of technical design can serve to avoid the issue of cross-border recognition of electronic signatures.

Nevertheless, the discussion of the cross-border aspects of electronic signatures here is quite useful when contemplating the design of a SW facility that encompasses the broader range of trade facilitation legal issues in a paperless trading environment as some countries have done or are currently considering, such as the Republic of Korea. This could include many benefits in the longer term in areas such as the electronic transferability of rights in goods (e.g., electronic bills of lading) that will help facilitate paperless trade in the global supply chain. From this perspective, therefore, these issues should be considered as part of the development planning of a SW.

In this context, at least two legislative approaches have been suggested. The first approach is based on local validation of foreign electronic signatures, often matched with a reciprocity mechanism. Under this approach, the legal validity of the signature depends on its place of origin. For instance, under the mechanism set forth in article 7 of the European Union directive on electronic signatures, signatures certified by a certification service provider established outside the European Union are recognized as legally equivalent to

[45] A detailed discussion of the topic is available in UNCITRAL, Promoting confidence in electronic commerce: legal issues on international use of electronic authentication and signature methods, Vienna, 2009, United Nations Publication Sales No. E.09.V.4.

certificates issued by a certification service provider established in the European Union if the foreign certification service provider receives accreditation in a Member State, or if its certificate is guaranteed by a certification service provider established within the Union. The possibility of recognition by virtue of a bilateral or multilateral international agreement is also envisaged.

The second approach disregards the place of origin as a relevant factor and builds on the substantive equivalence between domestic signatures and the foreign signature whose legal validity is at stake. In this line, article 12 of the UNCITRAL Model Law on Electronic Signatures points at the substantial equivalent level of reliability as a criterion for crossborder recognition of electronic signatures. In practice, this approach requires a comparison between the foreign signature and the closest corresponding domestic signature, but does not demand perfect identity between the two. Contractual agreements on mutual recognition of electronic signatures may also be relevant within the limits permissible under applicable law. If national law applies, this discussion assumes that this provision of the Model Law has been incorporated into applicable domestic law.

Recently, the matter has been dealt with in the framework of the ECC. Article 9, paragraph 3 of that Convention deals with the requirements for cross-border recognition of an electronic signature based on the general principles inspiring UNCITRAL texts. Namely, this provision establishes general conditions under which electronic signatures would be enforceable by requiring the use of a method that identifies the originator of an electronic communication, indicates the originator's intention in respect of the information contained in the electronic communication and provides an adequate level of reliability. This provision is strictly technologically neutral and independent of the place of origin of the electronic signature. If a State becomes a party to the Convention, this provision could operate as an enabler also for the legal recognition of some or all electronic signatures exchanged in the context of a crossborder electronic single window facility. *In fact, being contained in a treaty, this provision pre-empts the application of national law.*

D. Data quality, protection, retention issues and access to data

a. Data Quality Regulations

Data quality, i.e., the integrity or completeness and accuracy of the data or information, is critical in the SW for many reasons. For example, if valuation or origin information is incorrectly entered (that is, there is a data input error) on an electronic declaration, this might have an impact on duties or taxes to be assessed. Thus, the data input must be *accurate* and errors avoided. The *integrity* of the data input, that is, that data are complete (no data are missing) is also important. Therefore, it is necessary to establish controls over the data input process as well as responsibility for data entry and processing within the SW. Proper audit trails and recording mechanisms for this should be established in regulations for SW operations.

These regulations would provide guidelines for data entry and responsibility for errors submitted on electronic forms to the SW as well as subsequent processing of data within the SW. It may also be useful to develop

FURTHER READING

"Recommendations on Electronic Authentication and OECD-Guidance for Electronic Authentication", OECD (2007). Available at http://www.oecd.org/dataoecd/32/45/38921342.pdf

"Promoting Confidence in Electronic Commerce: Legal Issues on the International Use of Electronic Authentication and Signature Methods", UNCITRAL (2009). Available at http://www.uncitral.org/pdf/english/texts/electcom/08-55698_Ebook.pdf

regulations for error correction in the event that incorrect data are submitted by, for example, a trader or broker,[46] or where there has been a data input error made within customs or another government organizations accessing the SW.

Finally, it would be important to consider how to deal with these issues if the SW was organized as a "public-private partnership", under which the responsibility for operating the SW might be delegated to a private sector company. For example, matters related to data quality as well as other operational obligations could be established in the contract or concession agreement.

b. Data Protection and Information Security

UN/CEFACT Recommendation 35 includes a discussion of the issue of data protection or protecting information and data within the SW from unauthorized access or dissemination, and notes that this is of vital importance. While not minimizing its importance in the national SW environment, data protection may be particularly important in any cross-border SW environments. On the legal dimension, issues of information security (for example, the various technical measures for protecting information and data) and data protection intersect with those related to trade confidentiality and privacy laws.

There are several aspects of data protection that should be considered. First is the question of what data and information need to be protected or secured and second is the issue of what types of information security measures could be implemented to protect that data and information. Regarding what information needs to be protected, a SW is likely to process sensitive data and information. For example, an electronic SW may contain personally identifiable information (PII), trade-sensitive data, confidential business information, and possibly information related to national security. It may also have trade secret information about traders and companies participating in the system, as well as private data for banks, insurers, and other parties.[47]

As a SW develops over time, it may also contain financial information[48] used in connection with the collection of duties, taxes, and fees. It may also contain sensitive (and even classified) law enforcement information used primarily by government officials to enforce a wide variety of civil and criminal laws enacted for a broad range of purposes from ensuring food safety and public health to combating terrorism, money laundering and narcotics trafficking. Thus, ensuring appropriate protection of this type of data and information is fundamental to protecting the information assets of the government as well as private sector participants in the SW.

A SW should provide information security protections that are commensurate with the risk and magnitude of the harm resulting from the unauthorized access, use, disclosure, theft or loss of sensitive information collected or used in the system. Thus, it is important that the SW laws include, for example, laws that criminalize unauthorized access, and regulations that provide for appropriate security features to be in place to protect the SW facility.[49]

In order to design appropriate security for the SW, it is necessary to first assess the security risks to the system. This can be done by analysing:

Vulnerabilities — weaknesses that may be exploited

Threats — events or actions that may cause harm

[46] The types of errors contemplated here are simply unintentional errors, that is, they do not amount to attempt to commit fraud or other violations of national laws.

[47] See, L. Thomson, Legal Infrastructure Issues in Privacy, Information Security and Information Sharing Practical Steps for the Development a Secure Trade Data System, presented at the 6th Meeting of the ASW Working Group on Legal & Regulatory Matters, Da Lat, Viet Nam (16-17 February 2009), at pages 4-5.

[48] Some Single Window facilities have regulations dealing with the electronic payment of duties, fees and taxes associated with transactions processed through the SW.

[49] It may also be noted that countries may have broader computer or cyber-security laws that while not specifically dealing with the SW, would be applicable to the SW.

Risks — the probability that a threat will exploit a vulnerability with resulting damage

Countermeasures — actions, e.g. technology or procedure, that reduce or eliminate vulnerabilities or threats.

While this type of analysis is usually employed from a technical perspective, it is useful for those drafting the regulations for the SW to work with the systems developers and other government organizations to ensure that the information security needed to protect data and information processed in the SW meet international legal standards and best practices. The types of information security needs for the SW should include a variety of considerations. For example some of the general categories of issues being incorporated into the laws of some countries on data protection and that reflect emerging best practices are:

- Establish secure user authentication protocols. Implement secure access control measures that restrict access to personal and confidential information to those who need such access to perform their duties related to the SW.
- To the extent technically feasible, encrypt all records and files containing such data or information that will travel across public networks (i.e., open Internet networks) and encrypt all data that may be transmitted wirelessly.
- Monitor systems for unauthorized use of or access to personal or other sensitive trade data.
- Encrypt all information stored on laptop computers or other portable devises (e.g., small thumb drive devices.)
- Utilize firewall and operating system security patches that are reasonably designed to maintain the integrity of the data and information.
- Use regularly updated versions of system security agent software that includes protection against viruses and malware.
- Provide education and training for all SW and government employees who access the SW on the proper use of computer security systems and the importance of information security.[50]

These represent just a sample of the issues that should be addressed in the data protection and information security area for SW regulations. And since employees of other government organizations may also have access to or receive information from the SW, these regulations should apply to those organizations as well. For example, one approach would be to establish what are commonly called memoranda of understanding (MOUs), as well as information security agreements (ISAs) between the operator of the SW and other government organizations that would incorporate these types of requirements. In most discussions involving SWs, it becomes clear that issues of data protection and information security are critical to the operation of a SW.

c. Data Privacy

As noted above, part of data protection is concerned with "privacy" issues. As noted in Annex II of the UN/CEFACT Recommendation 35,

> *The issue of data protection is closely related to that of privacy (e.g., personal data protection) as well as the protection of proprietary company data and confidential trade data. When personal data are processed by a Single Window facility it must be determined whether this is in compliance with all relevant data protection laws.*
>
> *Some national legal regimes may distinguish between "privacy" issues; particularly those related to personally identifiable information and "confidentiality" issues related to both*

[50] Thomson, L., Editor, Data Breach and Encryption Handbook, pages 110-111 (American Bar Association 2011).

trade data and business information. Governments may wish to consider how these two areas should be addressed nationally and in the cross border environments. In this regard, the adoption of international legal standards and best practices is advisable.

Countries (and sometimes regions, for example, the European Union) that have strong privacy and trade confidentiality laws will likely consider the legal protections, as well as technical security measures, in deciding on whether to engage in SW transactions with a particular country. Therefore, not focusing on these data protections and information security issues in the legal and technical frameworks for a SW may create difficulties in linking the SW of various countries.

It should also be noted that many countries are increasingly working towards the development of general data privacy legal regimes. Besides the European Union, where such frameworks are already in place, there is the Asia-Pacific Economic Cooperation (APEC)'s Cross-border Privacy Enforcement Arrangement.[51] This arrangement is a result of a data privacy pathfinder initiative initiated in 2007 and is generally based on the Organization for Economic Development and Cooperation (OECD) Guidelines on Data Privacy.[52]

d. Data Retention and Electronic Archiving

In the paper environment for customs operations, retaining records and filings is an important aspect of customs administration and enforcement. This is no less important in the electronic environment and all of the foregoing issues related to the electronic SW will be relevant. Not only technical aspects, but also legal aspects of data protection and information security need to be addressed. That is, ensuring that archived data are secure and maintained in a form and format that will be legally enforceable at a later date is essential.

Establishing the necessary regulatory framework for data retention and electronic archiving anticipates decisions on a number of legal issues. For example, many countries have established data retention schedules for certain types of information. This includes distinctions between data related to regulatory filings and data involving personally identifiable information. In the latter case, governments will sometimes define the maximum time for which such data may be retained and then require that it be destroyed. It is possible that some countries already have certain criteria for retention of information and data in the paper environment for their Customs Administrations as well as for other government data collection activities. And depending on national policies, these criteria could also be adapted to the electronic environment of a SW.

Electronic archiving, i.e., the storage of electronic data and information, covers a wide range of areas. For example, it includes definition of the formats in which data will be stored, the requirements of national law, such as "original documents" that might be needed for subsequent use in an enforcement proceeding or in relation to possible civil disputes or, on a short timeframe, in Customs post-clearance audit procedures (see Box II.5).[53] An important issue here will be the choice of the technology utilized for data storage, which will be based on the legal requirements for its subsequent use, for example, as evidence in a legal proceeding.

Electronic transactions laws may contain provisions dealing with the storage of electronic documents. For example, some define the conditions for the electronic storage, such as accessibility without changes, maintaining the original format, and information regarding the date and time as well as place of sending and receipt. It is useful if such laws provide that electronic information and documents may be used as evidence and how verification, reliability, the method of

[51] See:http://www.apec.org/Groups/Committee-on-Trade-and-Investment/Electronic-Commerce-Steering-Group/Cross-border-Privacy-Enforcement-Arrangement.aspx

[52] OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data (1980).

[53] See also UNCITRAL Model Law on Electronic Commerce, art. 9(2): "Information in the form of a data message shall be given due evidential weight. In assessing the evidential weight of a data message, regard shall be had to the reliability of the manner in which the data message was gene rated, stored or communicated, to the reliability of the manner in which the integrity of the information was maintained, to the manner in which its originator was identified, and to any other relevant factor."

storage, etc., will be assessed in giving weight to electronic evidence in any proceeding. As mentioned above, it is recommended that the SW should use the same fundamental legal principles applicable to purely commercial (B2B) transactions.

Dealing with the electronic storage of "original documents" is important, that is, establishing the criteria for maintaining an electronic document in its original version. These should address (1) reliability as to the completeness of the document, (2) accessibility of the document for subsequent presentation, and (3) integrity of the document, i.e., assurances that there have been no changes in the document since its creation other than amendments or addendum as well as those notations that may occur in the ordinary course of transmission and storage.[54]

SW regulations should take into account these legal criteria as well as the technical requirements for achieving the desired storage and archiving. As a starting point, regulations for the SW could be established that are flexible and enabling so that if changes are required by, for example, advances in technology or other cross-border SW agreements, the SW can be quickly adapted by changes in its regulations to meet those needs.

Finally, these regulations should require that information and data exchanged with other SWs in the cross-border environment be retained and stored effectively in the event that there is a dispute regarding the underlying transaction processed by the SWs involved.

e. Access to and Sharing of Single Window Data

Law and regulations providing for the access to and sharing of customs and trade data information between government agencies and ministries should be addressed. For example, it is not always clear whether one governmental organization is permitted to share data and information with another

BOX II.5. Electronic archiving in the Republic of Korea

The Republic of Korea created the e-Trade Document Repository as a part of its U-Trade Hub SW facility for the purpose of archiving electronic trade documents. The Repository was created following the enactment of the Electronic Trade Facilitation Act (2005) in order to safely and reliably store the electronic documents processed by the SW.

The major functions of the Repository are to: (1) manage the electronic trade documents throughout their life-cycle from registration to deletion; (2) provide verification of the authenticity, integrity and status of electronic trade documents; (3) process and deliver electronic trade documents to third parties including relevant institutions such as banks and (4) provide statistics and information on the history and use of electronic trade documents. The E-Trade Facilitation Act further enforces trade-related institutions to submit 10 different kinds of documents to the Repository. The list includes: certificates of origin, international letters of credit, national letters of credit, letters of guarantee, delivery orders, insurance policies, import licenses, export licenses, trade approvals and purchase confirmations.

Documents submitted to U-Trade-Hub are automatically stored in the Repository with verification of authenticity of the original copy. Documents stored in the Repository are accepted as original copies and they can be used for electronic circulation by authorized personnel of the trading companies. Electronic circulation allows for facilitated distribution of trade documents to relevant institutions and third parties without the need to submit paper documents.

Source: https://www.utradehub.or.kr/porgw/english/html/eng_architecture_03.html

[54] See UNCITRAL Model Law on Electronic Commerce, art. 10: "Retention of data messages".

or, conversely, to provide such information to another governmental organization if requested to do so in a SW environment. Further, privacy or confidentiality laws or regulations in some countries prohibit the sharing of certain types of information between government organizations except when permitted by law.

These issues should also be reviewed in the context of possible cross-border transactions. In many countries, access and sharing considerations related to the SW have had to be authorized in national law before information can be shared or exchanged with another customs administration. It will be important to other customs administrations with which information and data may be shared that data sharing is legally permitted within a SW to ensure that transactions processed through that SW have legal validity.

Within a country's own SW environment, i.e., where Customs and other government organizations interoperate with the SW, it may be possible, as noted earlier, to manage these interactions through the use of inter-agency agreements such as Memoranda of Understanding and Interconnection Security Agreements (ISAs)[55] that have been established under applicable regulations for such information exchanges between government ministries or organizations. However, when drafting enabling legislation for a SW, the possibility of authorizing access and sharing of data should be considered to the extent possible. Where appropriate and in the context of the specific model developed for the SW, a process may then be established, possibly by regulations in each appropriate gover government organization, to implement sharing of relevant data in the SW.[56]

A further aspect of this issue is authorizing private sector entities (such as traders and customs brokers) to access the SW. For example, it will be necessary to permit such entities to connect electronically with the SW for purposes of submitting electronic documents for processing, arranging electronic payments for duties, taxes, and other fees, etc. Naturally, the procedures for such access should be governed by appropriate regulations and should include all of the requirements (for example, those for identification, authentication and authorization, electronic signatures, data protection and security, etc.) noted above.

E. Other Legal Issues

a. Legal Liability and Dispute Resolution

There are a number of ways in which potential liability[57] can arise within the SW environment. For example, errors in data input can create liability for traders utilizing the SW and that liability may result in other countries where the data from the SW are used. Such errors could be related to valuations, certificates of origin, certain import or export licenses or permits, and so on.

FURTHER READING

"Guidelines for the Regulation of Computerized Personal Data Files", UN General Assembly (1990). Available at: http://www.unhcr.org/ref-world/docid/3ddcafaac.html

"OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data" (1980).

Available at: http://www.uhoh.org/oecd-privacy-personal-data.PDF.

[55] Typically, Interconnection Security Agreements, or ISAs, in the Single Window environment are agreements between government ministries and the SW that establish the technical requirements for each participating ministry or government agency to connect to the SW. The 'technical requirements' usually deal with, among other matters, systems connectivity, information security requirements, and so on.

[56] It should be noted that not all technical designs for implementing a SW would need such authorization. For example, Singapore's TradeNet Single Window is designed so that explicit authorization is not required and, in most cases, there is no sharing of data between Ministries. In countries implementing various versions of ASYCUDA, such authorization may be needed. Thus, it is useful to include these issues specifically.

[57] In this section, only civil liability issues are discussed. Criminal and related customs enforcement activities, while undoubtedly covered in the existing laws of most countries and very important, are beyond the scope of the analysis in this *Guide*. However, the principles related to electronic transactions will apply in these areas as well.

Another way in which liability can arise in the operation of the SW is, for example, from delays resulting in the SW being "out-of-service". This could delay release of goods that are time-sensitive either under the contract between private parties or as related to the goods themselves, such as spoilage of perishable food shipments. To the extent that the SW is operated by a private sector entity (under a contract with the government) or as a public-private partnership, not meeting performance standards (including "system availability targets", i.e., the percentage of time the system must be operating during a certain time frame), liability may arise either for the operator or for the government.

Further, liability may arise from some forms of data breaches, that is, where external agents have illegally gained access to the SW and stolen or otherwise compromised confidential information and data. While criminal, administrative and civil sanctions may apply to these "hackers", there may still be civil liability on the part of the SW operator, should it be proved in a legal dispute that the damages that resulted to, for example, private sector traders, could have been avoided if the proper data protection and security methods had been employed by the SW.

Finally and from an international perspective, there may be performance criteria established under regional SW environments that will need to be met, for example, in the area of SW system availability in each participating SW. These criteria may set a different and possibly higher standard as liability benchmark. It is likely that regional SW initiatives will be governed by some Agreement between participating States and care should be taken in negotiating this aspect of such Agreements.[58]

It should be noted that the issue of liability for damages arising from the operation of an international SW facility would need to take into account also the national laws and policy considerations of the countries involved. It will be important to consider how national law would operate in these circumstances and determine whether some appropriate methods should be established for limiting this liability. For example, if the SW uses legal agreements (e.g., "end-user agreements") with traders who utilize the SW, it may be possible to limit government liability for such errors or to create an indemnity system of some type to deal with this.

It is important to note that the establishment of a SW does not, *per se*, affect the liability regime of its participants with respect those actions or omissions occurring during customs operations or other related transactions. Thus, for instance, the intentionally incorrect submission of information will be punished under criminal, administrative and civil law, as in the paper-based system. However, the electronic nature of the facility may require specific measures for evidence taking. At the same time, the automated recording and storing of all interactions with the SW may result in more effective data collection, monitoring and, eventually, enforcement. In this respect, the implementation of electronic means may provide an opportunity for assessing, and, if need be, improving the liability regime through the legal gap analysis.

It is also important to consider alternative dispute resolution (ADR) mechanisms to deal with liability issues that may arise. Given the length of litigation in many countries, there may be significant time advantages to establishing some types of mediation and/or binding arbitration arrangements in which these types of claims can be settled expeditiously. Other potential benefits of ADR pertain to confidentiality of proceedings. Additionally, these types of ADR agreements may be particularly valuable where potential liability arises outside of a country and legal jurisdiction of the dispute is in another country.

[58] For example, the ASEAN Single Window project is considering a 'legal framework agreement' in which it is anticipated that issues related to this type of liability may be addressed.

b. Intellectual Property Rights and Database Ownership

Intellectual property rights (IPR) issues may arise in the context of the SW in two cases. First are those related to "ownership" of the data that are in the SW and what IPR content that "ownership" has. For example, if a trader submits information electronically to the SW,

presumably the trader owns that information and, depending on the commercial confidentiality and privacy rules in national law, that information should remain confidential to that trader.

At the same time, the government may also have ownership rights in the databases that are maintained in the SW. As a result, careful attention must also be paid to those situations in which private or quasi-private sector entities operate a SW. For example, if a government contracted with such a party, the contract to operate the SW should reserve all ownership rights in the information and data in, or related to, the SW to the government.

A second set of IPR issues relate to the actual development of the SW, including all of the computer hardware, software, firmware, etc., associated with the SW.[59] There may be other IPR considerations related to the overall systems aspects of the SW. For example, IPR issues often arise when a third-party software developer or a vendor providing systems hardware provides products or services for SW. One question is who "owns" the software that is developed under a software development contract. Many times developers wish to retain ownership of the software and provide a license to the user.

License agreements may vary considerably. Some provide that only the developer can make changes to the software, which would "lock" the government into using only that developer when changes and improvements are needed. Other licenses state that if a user makes some special modification or upgrade to the software, the developer owns the rights to those modifications and may use and license them to others. Thus, careful attention needs to be placed on the terms of any license agreements for developing components of the SW.

Additionally, careful attention must be paid to the warranties that are provided with both software and hardware that are sold or licensed to the SW. For example, it is important to have warranties from the vendor or developer stating that it is the sole owner of the IPR related to the software or hardware and that it will indemnify the government for any claims made against it by third-parties, for example, for patent infringement. Such indemnities should cover possible damages as well as litigation costs whether the claim succeeds or not. Naturally, not all vendors will agree to all of these terms, so a process of negotiation may be needed. But it is important to look at these issues when embarking on the development of the SW.

c. Service Level Agreements[60]

Service Level Agreement (SLA) is the term commonly used to refer to the portion of a vendor service agreement or an outsourcing agreement dealing with quantitative performance metrics. It can also refer to an entire vendor agreement in which issues of performance and performance measurement form the core of the agreement. SLAs can be very complex, since they are meant to measure and address the quality of the service provided, and to establish benchmarks, guarantees and/or payment levels based on that level of quality. They also commonly address the difficult issue of contingency processing.

SLAs can be established with both purely outsourced SW facilities (that is, a private sector entity operates the SW for the government) or where a Public-Private Partnership (PPP) operates the SW. Because

[59] For those countries using ASYCUDA, "total ownership of the system and of all further developments by the user-country or organization" is provided. See, http://www.asycuda.org/awbenefits.asp.

[60] This sections and the next draws heavily on Field, Richard, "ASEAN Single Window: Introduction to Service Level (and Related) Agreements", Working Paper, Sixth Meeting of the ASW Working Group on Legal & Regulatory Matters Da Lat, Viet Nam – 16-17 February, 2009. The paper was funded as part of a U.S. Agency for International Development (USAID) ASEAN Single Window Project, which is part of the ADVANCE Program supported by USAID and the U.S. Department of State managed by Nathan Associates, Inc.

service levels are specific to the type of services to be outsourced, as well as the needs of the SW facility, there is no standard formula for service levels. However, there are a number of typical issues commonly dealt with in SLAs and it is not difficult on the Internet to find many "template" services for SLAs – essentially boilerplate agreements that can be used "as is" or edited by lawyers to address actual situations.

SLAs usually set out reasonable goals for both parties, while helping to reduce conflict and define priorities. They also provide motivation for service providers to meet or exceed standards, and appropriate penalties for failure to meet them. The core issues dealt with in SLAs are the quantitative aspects of or metrics for the services to be performed. These may be set out in one or more Schedules to the SLA. Box II.6 lists some of the issues that should be considered for inclusion in a SLA.

The list shown in Box II.6 is not all-inclusive. There may be any number of additional concerns, e.g., invoicing and taxes, force majeure, limitations of liability, non-hire of employees, and more. Some of the issues, such as privacy, security, IP and others, will likely require a more extensive focus than others. However, this list is meant to introduce, in broad terms, the principal issues that should be addressed in connection with SLAs.

BOX II.6. List of issues to be considered in service level agreements (SLAs)

1). Scope of services to be performed, including definitions of services. These services will vary depending on the system. Common services may entail:
   a. System and/or software development services;
   b. System and/or software maintenance services;
   c. Network hosting/virtual private network services
   d. Transactional services; call center services; etc.
2). Testing.
3). Measures of service levels / reporting of service level metrics / vendor auditing, third party audits, system owner access to audit data, automation of metrics data.
4). Warranties relating to adherence to service levels.
5). Compensation for services; payment bonuses/penalties for early/late performance.
6). Problem management.
7). Contingency processing / disaster recovery / access to premises.
8). Responsibilities of the system owner.
9). Maintenance windows.
10). Notification of planned/unexpected downtime.
11). Termination of agreement / transition to new service provider.
12). Compliance with applicable law and regulation.
13). Dispute resolution / submission to jurisdiction.
14). Privacy concerns.
15). Security concerns.
16). Intellectual property issues and ownership of physical property, inventions, software and software developments, data, etc.
17). Confidentiality.

Source: Attorney Richard Field, "ASEAN Single Window: Introduction to Service Level (and Related) Agreements" (2009).

A further consideration is that, for services not requiring a response to a unique Request for Proposal, it is likely that vendors will have their own proposed agreements, which may include many of the service level and related issues described above. A vendor's expertise can be quite useful in helping define needs and solutions. However, it should be anticipated that a standard vendor agreement or proposal would focus primarily on those issues of benefit to the vendor.

Special care should be taken, in any legal review as well as any business or technical review, to determine what issues of importance to the SW have been minimized or left out entirely. Issues often not adequately addressed by vendors may include confidentiality, privacy and security, warranties (including IPR issues) and remedies for breach, auditing, procedures on termination, indemnifications, and contingency processing.

Finally, one cannot consider SLAs without first understanding the architecture of the SW system, what needs to be produced, and what concerns exist with respect to timeliness and criticality of services. Individual SLAs and other service agreements will vary substantially. While there are common issues addressed in most SLAs, the goal of any SLA is to obtain just what is needed, with sufficient confidence, and at a suitable cost.

d. End-User License Agreements (EULA) or Terms of Use Agreement

Agreements with those private sector entities (traders, brokers, agents, etc.) who may have access to the SW for purposes of filing documents, requesting licenses and permits, and for receiving notices of decisions from the SW should be developed. The Agreement may be fashioned as a license to access or just a user agreement.

National law generally governs contracts of this type. The agreement can cover a wide variety of areas related to the end-users access to the SW. The items listed in Box II.7 illustrate just a few of these areas.

BOX II.7. Sample of areas that might be covered in end-user agreements

1). The level of the access for which the user will be authorized;
2). The obligations that the user and the SW will have regarding the SW;
3). Limitations on usage (if appropriate) such as the times during which the SW will be available for submissions (e.g., between certain hours each day, certain days each week, 24/7, etc.);
4). User's access procedures and security codes (e.g., user id and password);
5). Explanation of the importance of maintaining agreed security procedures;
6). Reporting requirements for actual or potential security infringements, and any penalties or fees associated with those infringements;
7). Error correction procedures;
8). Conditions for suspending or cancelling a user's access;
9). Limitations of liability for SW errors or unavailability (if admissible under applicable law;
10). Alternative dispute resolution requirements and processes;
11). Ownership of information that is provided to the SW;
12). Any IPR requirements that might apply;
13). Confidentiality requirements of the user as well as those of the SW;
14). A schedule of fees and other costs that may be assessed for access to the SW as well as the acceptable payment methods that may be used;

Part 3:
Mini-Case Studies

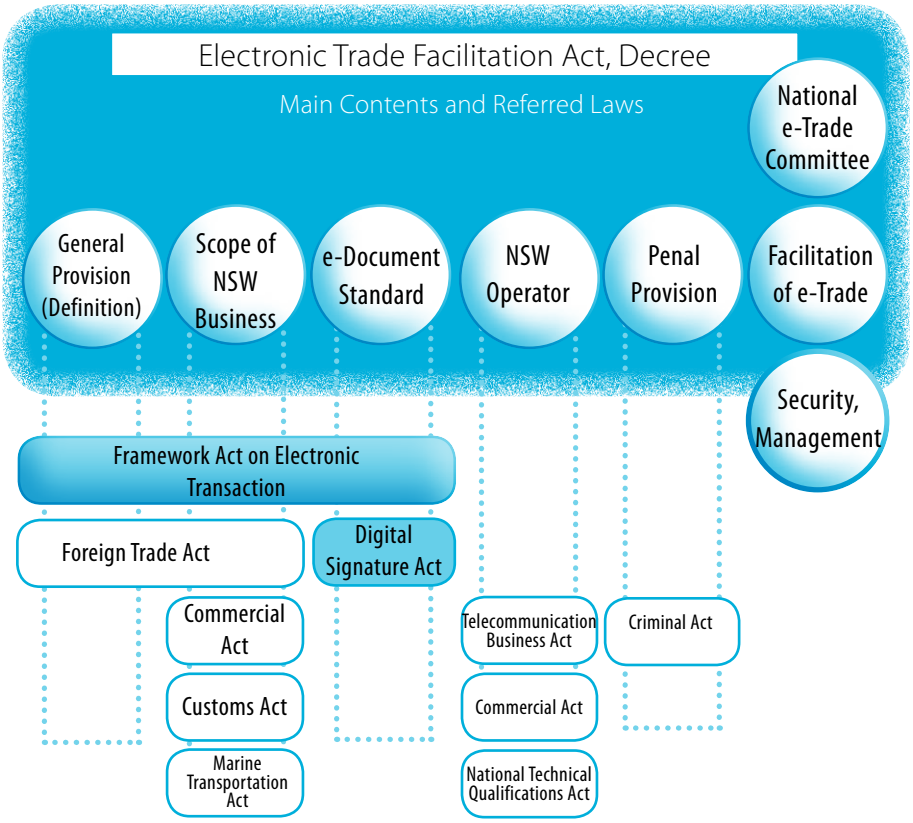
A. Mini-Case Study I: The Legal Framework of the Republic of Korea National Single Window

a. Background and History of the Legal Framework

The Republic of Korea enacted the Act on the Promotion of Office Automation for Trade in December 1991 to enhance the competitiveness of the trade industry by promoting office automation for trade, introducing paperless trade services, and facilitating the use of electronic documents for trade business. As a result, EDI-based paperless trade systems were successfully developed and adopted in many trade-related agencies as well as by private trade service providers such as banks and insurance companies. The systems aimed at automating administrative processes resulting in making these processes more transparent and more efficient.

As new ICT technologies were introduced, such as web-based applications and digital signatures, the Republic of Korea enacted the Digital Signature Act and the Framework Act on Electronic Transaction in July 1999. These laws established the basic framework necessary to clarify the legal relations between parties involved in an electronic transaction, to secure the safety and reliability of electronic transactions (data messages) and to promote and stimulate the use of electronic records and communications on a national level for advancing social benefit and convenience. The Framework Act on Electronic Transaction was wholly amended in 2002 to further promote e-transactions and clarify legal relationship between parties. It also addressed customer protection and privacy issues in more detail.

Figure III.1. Overview of the legal framework for Single Window in the Republic of Korea



In December 2005, in response to the global trend encouraging the establishment of national SWs and to the rapid change of ICT environment, the Republic of Korea enacted the Electronic Trade Facilitation Act. This new Act wholly revised the Act on the Promotion of Office Automation for Trade and referred to the Framework Act on Electronic Transactions and Electronic Signature Act to address issues related to the life-cycle of e-documents and the need for an e-document depository. Figure III.1 shows how the Electronic Trade Facilitation Act builds upon and relates to other laws in the country.

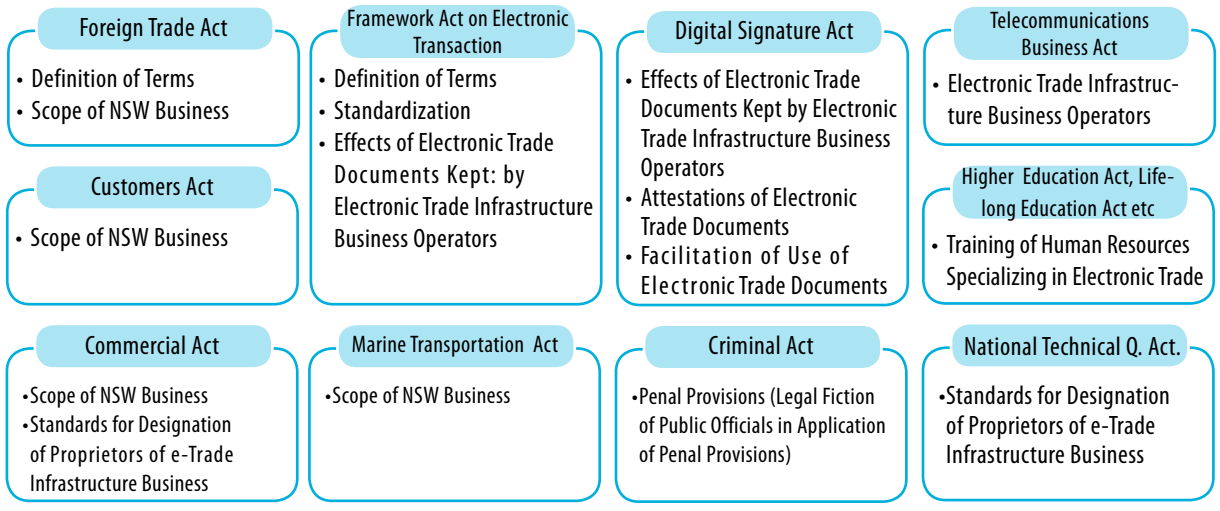
b. Functions of The Three Main Single Window-related Laws

The Electronic Trade Facilitation Act (1991, wholly amended 2005): This act enables the development and operation of the national electronic trade system in the Republic of Korea. It provides for the following:

- Facilitation of e-Trade including international cooperation, statistics, arbitration, financial resources
- Establishment of a National Electronic Trade Committee
- Security and management of electronic trade documents and trade information
- Facilitation of development of electronic trade techniques and training of human resources specializing in electronic trade
- Electronic trade infrastructure (National Single Window) business operators
- Scope of SW Business, Standardization of Electronic Trade Documents
- Keeping and attestations of electronic trade documents (legal effects of electronic trade documents kept by electronic trade infrastructure business operators)
- Facilitation of the use of electronic trade documents
- Penal provisions on wrongful acts related to e-trade

While this Act built upon relevant legislation, such as the Framework Act on Electronic Transaction and the Digital Signature Act, it also led to revisions and amendments to a number of other laws, such as the Customs Act (discussed in section c. below). Figure III.2 provides an overview of the content of various laws related to the e-Trade Facilitation Act.

Figure III.2. Other Acts and provisions related to the E-Trade Facilitation Act



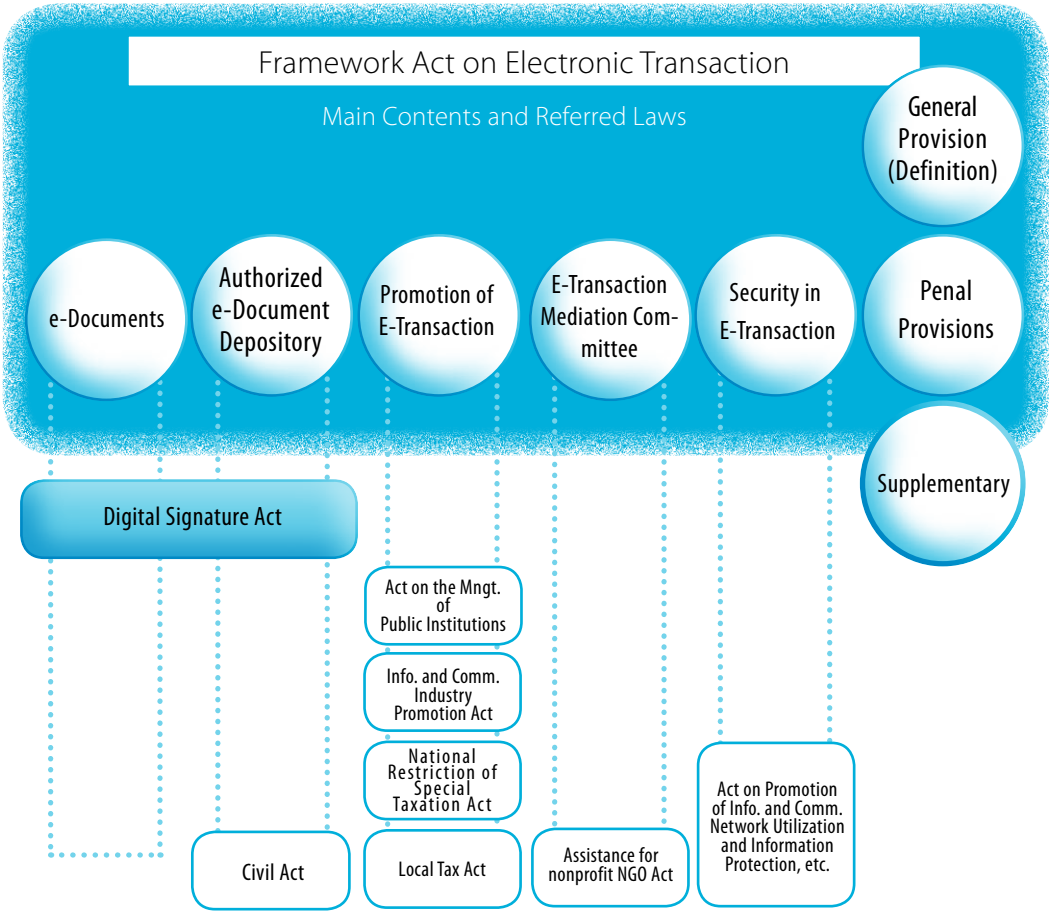
Note: NSW stands for national single window

The Framework Act on e-Transaction (1999, wholly amended 2002): This Act provides the legal basis for all electronic transactions in the Republic of Korea, including (but not limited to) international trade transactions. It provides for the following:

- The definition of electronic documents (validity; custody; time and place of transmission or receipt of e-documents; independency of e-document received; acknowledgement of receipt) and electronic transaction
- Security measures in e-transaction and protection of consumers such as protection of personal data and business secrets, rule and authentication for business operators of etransaction
- Promotion of e-transaction and use of e-documents including the establishment of institution promoting e-transaction, standardization and internalization of etransaction, survey on statistics of e-transaction
- Designation of Authorized Electronic Documents Depository and its business, effect of vicarious execution of keeping of e-documents, regulations on business of edocuments depository, security and protection of related information such as edocuments and users' information, and responsibility for indemnity.
- Establishment of E-Transaction Mediation Committee (mediation of disputes, operation of committee, etc.)

As shown in figure III.3, a significant number of provisions in this Act, including those related to the definition and authentication of electronic documents as well as the operation of the authorized electronic document repository, are related to the Digital Signature Act.

Figure III.3. Features of the Act on Electronic Transactions



The Digital Signature Act (1999): This Act provides for the following:

- Definition of digital signature, and provisions on the effect of digital signature, issuance/ termination/ validity of authorized certificate, personal identification by authorized certificate,
- Licensed Certificate Authority (designation, certificate service)
- Security measures (Control of Digital Signature and its Creating Key, Record of Certification, Protection of Information on Individual) as well as Time Stamp of Electronic Messages
- Mutual recognition of digital signatures among licensed CAs, training of human resources and development of techniques, promotion of digital signatures
- Reciprocal recognition (Agreement) of digital signatures with foreign governments

c. Customs Law Provisions for Electronic Trade and Single Window

When Korea Customs Service (KCS) established its automated system, KCS had to amend and update several provisions of the then existing Customs Law in order to enable Customs to work with the automated data in lieu of paper based declarations. The first amendments were on the definition of the "time of acceptance of declaration" and "time of approval of declaration", because it was a technically important element in deciding the applicable tax rate and exchange rate, and calculation of due date of tax payment.

As mentioned earlier, the issuance of the e-Trade Facilitation Act has had implications for the operations of various agencies, including KCS. Currently, KCS has up-to-date Customs laws and regulations, which consist of the following legislative instruments.[61]

Customs Law and Enforcement Decree	Key provisions
Article 226 and Article 233 of Enforcement Decree	• Customs authority to check other government agencies (OGA)' requirements; and empowering Customs to do it by electronic means
Article 245	• Business can be exempted from submitting import/export declarations and supporting documents
Article 254	• Special provisions on importing/exporting through e-commerce
Article 255-3	• Authorizing Customs to exchange data with other Customs administration
Article 327	• Authorizing Commissioner of Customs to operate national SW system • Authorizing Customs to handle import/export declaration with data • Simplified Customs procedures for SW • Time of acceptance and approval • E-delivery of Customs decision
Article 327-2, 327-3, 327-4	• Authority of Commissioner of Customs to decide the SW operator • Selection criteria and penalties for the SW operator • Security and liable person • Authority of Commissioner of Customs to set the data and communication standards

[61] For full text of the Korean Customs Law please visit its website at: http://english.customs.go.kr/kcshome/site/index.do?layoutSiteId=english

B. Mini-Case Study II: The Legal Framework of the Singapore National Single Window[62]

a. Operational Background of TradeNet

Singapore's TradeNet was established in 1989 as an electronic data interchange system allowing public and private parties to exchange trade messages and information electronically.[63] TradeNet is arguably the world's first electronic B2G filing system for documents related to import and export activities.

The development of TradeNet was led by the Singapore Trade Development Board (STDB), the government agency responsible for trade facilitation and now known as International Enterprise Singapore (IE Singapore), in close collaboration with other governmental authorities involved in international trade transactions.

TradeNet was established as a Public-Private-Partnership (PPP) venture in order to enable Singapore to increase the involvement of the private sector in the delivery of public services aiming to provide an effective and low-cost service. [64] The decision to assign TradeNet's operations to a private company enabled the government to avoid costly investments in infrastructure and services and the direct costs of running and operating the SW system. The initial costs of establishing the service were an approximate US$12 million and currently the system is self-sustained by various fees.[65] In addition, the PPP approach has also enabled CrimsonLogic Pte, the private company operating TradeNet, to develop similar systems in other countries. The company has provided or provides similar services in, e.g., Mauritius, Qatar and Ghana.

Using TradeNet for the exchange of trade messages and information in Singapore became mandatory by late 1991 although more than 95% of the related trade documentation exchanged in Singapore were already handled within the SW by then.[66] TradeNet currently handles documentation serving over 8000 users who send more than 30,000 declarations daily. Since TradeNet's launch, the processing time per permit has been reduced from 2-7 days to one minute or less.[67] It is estimated that TradeNet generates an approximate annual savings of US$1 billion for Singapore's trading environment.[68]

b. The Legal Framework Behind TradeNet

Early development and current situation

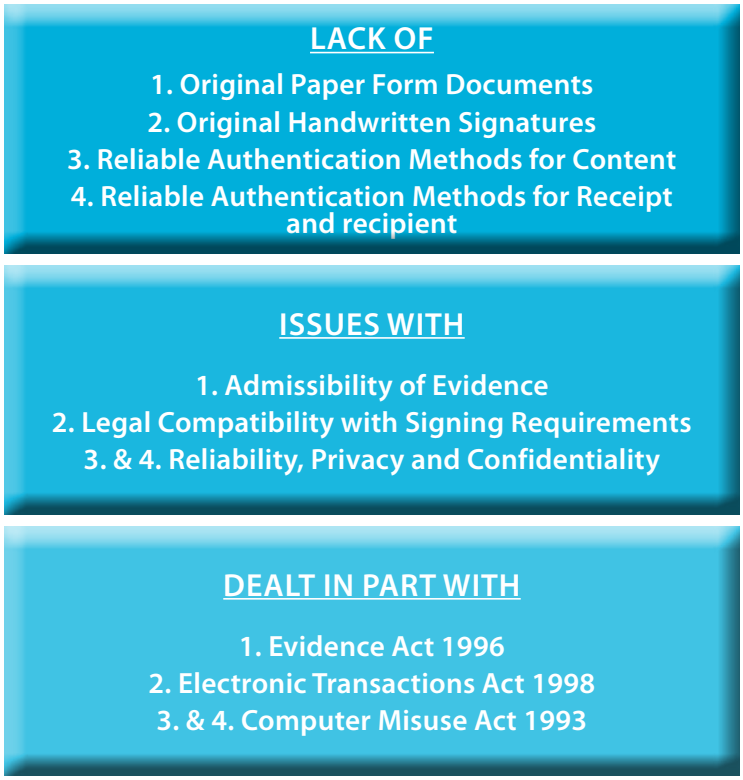
The legislative and regulatory development behind TradeNet is unique. As a trailblazer for creating a national SW facility like TradeNet, Singapore was forced to learn mostly from first-hand experiences and to pioneer legal approaches when mitigating the multifaceted legal issues presented when moving from a paper-based system to a paperless environment.

The legislative genesis spans the creation of acts such as the Computer Misuse Act (1993), the Evidence Act (1996), the Electronic Transactions Act (ETA, 1998, amended 2010) and the Customs Act, all of which containing important provisions that enable the seamless operation of TradeNet and other electronic commerce facilities (see Figure III.4). These provisions provide, e.g., authorization for governmental authorities to operate computer services and allow for the submitting and receiving various import/export related documents by electronic means. Additional legislative instruments set forth rules concerning data privacy and confidentiality issues.

[62] Adapted from UNNExT Occasional Paper Series, "Assessing the legal framework of Singapore's TradeNet", (2012).
[63] Asian Development Bank, "Singapore's TradeNet System", 2005, p. 1.
[64] Asia-Pacific Economic Cooperation (APEC), (2009), "Evolution of Singapore's Single Window." Single Window Working Group Capacity Building Workshop 4, Singapore, p. 7.
[65] Sathasivam, K., CrimsonLogic Pte., "The Single Electronic Window –Singapore's TradeNet –Scope of Services And Pricing Model", Singapore 2008, p. 27.
[66] APEC (2009), p. 33.
[67] Koh Tat Sen, Jonathan, Crimsonlogic Pte., "Blazing new trails" (2009), p. 4.
[68] See CrimsonLogic website: http://www.crimsonlogic.com/solutionsAndServices/governments/tradeFacilitation/

Figure III.4. Key legislative instruments supporting TradeNet operation

Figure III.5. Legal issues related to the use of TradeNet



Source: J. Chan Wah Teck, "Legal issues in e-commerce and electronic contracting: the Singapore Position."Asean Law Association. (2009), p.234

The above-mentioned acts form the enabling legal framework for paperless trade in Singapore. They are aimed at addressing various issues that arise from the lack of original paper form documents and handwritten signatures in electronic transactions, as well as the need for reliable authentication methods for preparing and sending electronic messages (content) and receiving them (see Figure III.5).

The Electronic Transactions Act of Singapore

The Electronic Transactions Act (ETA)[69] is the de facto backbone of the Singaporean paperless trade framework. The act was first introduced in 1998 and subsequently repealed and re-enacted in 2010. The act is based on the UNCITRAL Model Law on Electronic Commerce and thus it extensively covers the central issues concerning a well-functioning paperless trade environment. Its 2010 amendment allowed for the incorporation at the national level, and for the ratification at the international level, of the ECC. ETA was drafted and implemented as an output of a target-oriented process to develop effective national legislation with full international compatibility.

ETA contains the necessary provisions for the legal recognition of electronic documents as full-fledged equivalents for written documents, which in turn enables TradeNet to function with full regulatory and legislative compliance when dealing with various notifications and declarations. The act also enables the more general e-commerce or paperless trade environment to function by allowing electronic documents to be used interchangeably with traditional paper documents, inherently facilitating the integration of B2G and B2B systems. The ETA also stipulates extensively on the use of electronic signatures (See Box II.3 in this publication).

Singapore has also taken into account the importance of dealing with service provider liability issues within the information society in a very straightforward and innovationsupporting manner. To facilitate the current and future provision of network services, the ETA grants service providers with the immunity against criminal or civil liability in several situations. This immunity in turn lowers the risk and related costs for service providers operating within the electronic commerce environment, such as TradeNet.

SW facilities like TradeNet handle information and documents which often are used not only for import/export procedure purposes at the moment of processing but also for other purposes, e.g., as a basis for future legal proceedings or enforcement measures. Thus ETA provides for the use of electronic documents for data retention purposes in Section 9. In addition, Section 10 of the ETA has a specific provision on the requirements concerning the originality of electronic documents used.

Whereas data privacy and protection issues are dealt in more detail elsewhere in Singaporean legislation, the ETA does contain provisions in Section 28 which establish a direct obligation of confidentiality concerning electronic records.

c. Concluding Remarks

The Singaporean experience with TradeNet is a testimony to the fact that a proactive approach to trade facilitation by novel means and with a future-oriented attitude can lead to significant benefits for the national economy. Not only has TradeNet facilitated import/export procedures but its establishment has also been an important driver for crucial legal reforms which in turn have formed the enabling legal framework for e-commerce and paperless trade in general.

The standing of Singapore as a world leader in trade facilitation and paperless trade is easily explained by the will – and seemingly limitless capacity – of its government and private sector to innovate and prepare for future challenges (see Box I.2 in this publication). Singapore is actively taking part in the international development of trade facilitation methods and related legislative reforms, not only by using existing international standards, but also by shaping future ones. Singapore has clear intentions to make sure its laws enable the development of new and innovative services,[70] continuously and proactively searching for ways to clarify and apply e-commerce related legislations.[71]

[69] The statute can be accessed through the Singapore Statues Online service at http://statutes.agc.gov.sg/aol/home.w3p

[70] UNPAN, "Singapore's Legal and Policy Environment for E-commerce", (2010), p. 1.

[71] See Info-communications Development Authority of Singapore website: http://www.ida.gov.sg/Policies%20and%20Regulation/20060526123350.aspx

C. Mini-Case Study III: Legal Gap Analysis Towards a National Single Window in Lao People's Democratic Republic

a. Introduction

The Lao People's Democratic Republic is a member of the ten-nation Association of Southeast Asian Nations (ASEAN). Since at least the mid-2000s, ASEAN and its Member States have been working towards the development of a regional Single Window as an element of their overall economic integration strategy. In 2005, the ASEAN member States signed the ASEAN Single Window Agreement (ASW Agreement)[72] and in 2006, they entered into the ASEAN Single Window Protocol (ASW Protocol).[73]

In order to meet its obligations under the ASW Agreement, the Lao People's Democratic Republic has actively engaged in preparations for developing its SW. As part of these preparations, the Lao People's Democratic Republic requested assistance from the ASEAN Secretariat[74] in developing a legal analysis that focused on identifying potential gaps in the domestic legal framework to be addressed for the full implementation of the Lao People's Democratic Republic SW and its cross-border interoperability in an electronic environment with the ASEAN Single Window. The formal work on this project began in February 2011 and was completed in June 2011.

In addition to its goals with respect to the ASEAN Single Window, the Lao People's Democratic Republic, National ICT Policy recognized that ICT was becoming an increasingly important tool of socio-economic development. The National ICT Policy focuses on advancing Lao People's Democratic Republic capabilities in the information age and notes, among nine priority areas, the importance of development of an ICT legal framework to achieve its national goals.[75] The Policy places emphasis on various aspects for electronic commerce development and on the key role that a basic underlying electronic commerce legal framework will play. It is also expected that the legal framework governing e-Commerce and online transactions would be harmonized with international, regional and subregional frameworks.[76]

The legal review and analysis of the legal framework for establishing its SW was based on meetings held with Lao government officials and private sector legal advisors as well as the review of Lao legal materials. The final analysis identified the potential gaps in the Lao legal framework for establishing its SW, particularly those pertaining to the electronic environment in which the Lao People's Democratic Republic SW will operate, as well as those for the underlying legal framework for electronic commerce and transactions.

b. The Legal Framework Analysis

The analysis undertaken focused on determining what legal gaps the Lao People's Democratic Republic might need to address in two areas. First, the research examined the underlying legal framework for electronic transactions and second, it discussed those legal provisions needed to implement the national SW facility. As the country was committed to establishing an electronic SW, it was important to ensure that a solid electronic commerce law foundation was in place.

The research noted that Lao People's Democratic Republic already had some recent legislation that provided for the use of ICT modalities for e-government purposes. For example, the Law on Investment Promotion[77]

[72] Agreement to Establish and Implement the ASEAN Single Window, Kuala Lumpur, (9 December 2005) available at http://www.aseansec.org/18006.htm

[73] Protocol to Establish and Implement the ASEAN Single Window, (20 December 2006), available a http://www.aseansec.org/23084.pdf; see also, Vientiane Action Programme, (29 November 2004) available at http://www.aseansec.org/VAP-10th ASEAN Summit.pdf

[74] Assistance and support for this effort was provided by the USAID under its ASEAN Single Window Project, which is part of the ADVANCE Program supported by USAID and the U.S. Department of State managed by Nathan Associates Inc

[75] See, S. Kittingnavong, "ICT Development in Lao", United Nations Economic and Social Commission for Asia and the Pacific (UNESCAP), Expert Group Meeting on Regional Cooperation towards Building an Information. Society in Asia and the Pacific, 20-22 July 2009, Bangkok, Thailand, available at http://www.unescap.org/idd/events/2009_EGM-WSIS/

[76] See, S. PHOUYAVONG, "Country Report on Information Access and Media and Information Literacy: LAO" (PPT Presentation), the fifth Asia-Pacific Information Network (APIN) Meeting and ICT Literacy Workshop, 23-26 November 2010 Manila, Philippines

[77] Law on Investment Promotion, No. 02/NA, Vientiane, 8 July 2009

describes the use of the "one-door-service" for a variety of purposes provided for in the Law. Article 44 of this Law describes the one-doorservice, as:

> ***"The investment's one-door-service is the services which provide the facilities in all fields to the investors through the provision of services on data and information, consideration of the investment, issuance of enterprise registration certificate or concession license and the issuance of notifications relating to the investment."***[78]

In 2010, the Prime Minister of the Lao People's Democratic Republic signed the Decree on Special Economic Zone and Specific Economic Zones (Lao SEZ Decree).[79] This Decree, "… defines the principles, regulations, organization, activities, policies relating to the special economic zones and specific economic zones (SEZ), constituting the translation of the implementation of the Law on Investment Promotion…".[80] For purposes of the One-Door- Service concept, the Lao SEZ Decree contains a specific provision related to the use of ICT in the filing of an application. Article 27 provides that an individual or legal entity may submit an application for investment "on a determined form".This Article goes on to note that, "the Investor can submit the application for investment via facsimile, electronic mail, or by hand…." [*Emphasis added.*]

The use of this type of electronic "data message," [81] that is, an email, has significant implications for the development of an underlying ICT legal framework for the Lao People's Democratic Republic under any type of one-door-service or SW concept. In the case of the Law on Investment Promotion, for example, the applicant's submission of "a determined form" has converted that form to an "electronic" version of that paper form.

Also on the electronic commerce side, the Lao People's Democratic Republic was reviewing a new Electronic Transactions Law. This proposed law appears to be inspired by the UNCITRAL Model Law on Electronic Commerce and goes beyond the Model Law to include provisions related to e-Government. Regarding basic legal issues, this Law covers a variety of areas including:

- Functional equivalence of paper and electronic documents.
- The use of electronic documents and information as "evidence."
- Electronic storage and archiving requirements.
- Electronic signatures and certification authorities.
- Web-based transactions.
- The electronic transactions activities of government agencies.
- Contract formation elements including time and place of sending and receiving.
- A list of typical exceptions for certain transactions (e.g., land titles, house and fixed asset ownership certificates, and inheritance matters).

When enacted, this Law would provide the Lao People's Democratic Republic with a very sound electronic commerce foundation for its SW.

The research also examined those legal areas that were specifically related to legally enabling the Lao People's Democratic Republic SW. The Checklist of legal issues provided in (Annex **II)** of UN/CEFACT Recommendation 35 was used as the starting point for the analysis. The issues researched included, among others:

- Legal basis for implementing a Single Window facility
- SW facility structure and organization
- Data protection
- Authority to access and share data between government agencies
- Identification, authentication and authorization

[78] Id., Section 6 – Investment's One-Door-Service, Article 44.
[79] Decree on Special Economic Zone and Specific Economic Zone in Lao PDR.
[80] Id., Article 1 Objectives.
[81] It should be noted that Article 4(c) of the UN Electronic Communications Convention defines a data message as: "information generated, sent, received or stored by electronic, magnetic, optical or similar means, including, but not limited to, electronic data interchange, electronic mail, telegram, telex or telecopy."

- Data quality issues
- Liability issues (obligations and responsibility)
- Arbitration and dispute resolution
- Electronic documents*
- Electronic archiving and data retention*
- Electronic evidence*
- Intellectual property rights and database ownership
- Competition

Note: * Also considered as part of the electronic commerce analysis.

c. Recommendations and On-going Efforts

Based on this legal research, a series of key recommendations or priorities were developed. These included:

1. Implement a national Electronic Transactions Law based on international legal standards;
2. Create the necessary enabling legal infrastructure for the Lao People's Democratic Republic National Single Window, including:
    - Develop a *Prime Minister Decree to Establish and Operate a National Single Window*
    - Establish a drafting Committee with legal representation from appropriate Ministries
    - Incorporate UN/CEFACT Recommendation 35 principles
    - Accommodate cross-border transactions
    - Provide oversight for the development or modification of those regulations that may be needed to implement the *Decree;*
3. Involve Lao People's Democratic Republic lawyers and legal experts in the ASW Legal Working Group;
4. Initiate outreach activities within the Lao People's Democratic Republic legal and business communities regarding the legal framework for the SW;
5. Study the possible benefits to Lao People's Democratic Republic and the national SW of acceding to the UN Electronic Communications Convention and consider the application of Article 20 of the Convention to other International Agreements to which Lao People's Democratic Republic is a Contracting Party;
6. Develop a timetable for each task.

Since the final report was presented at a National Workshop in Vientiane, government officials have moved quickly to implement the recommendations in the report. The Lao People's Democratic Republic draft Electronic Transaction Law is being moved forward towards adoption. A Prime Minister's Decree has been drafted to authorize and enable the SW and to create the high-level governmental entities that will oversee and manage the development of the SW. A set of principles have been prepared that will guide the development and implementation of the necessary regulatory scheme for the SW. Consultations on the SW with both government and private sector parties throughout the country are underway.

Perhaps one of the most important factors in the progress the Lao People's Democratic Republic has made in moving its SW forward has been the foresight and commitment of senior government officials. As a result, the Lao People's Democratic Republic is well on its way towards meeting its commitments to the ASEAN Single Window project and also to achieving its longer-term goals for trade and development.

FURTHER READING

"Lao PDR Single Window Implementation: Legal Requirements, Analysis, and Recommendations, Final Report", Consultant for USAID ASEAN Single Window Project, which is part of the ADVANCE Program supported by USAID and the U.S. Department of State (2011). Available at http://advanceiqc.com/uploads/lao-pdr-sw-legal-gap-analysis-final-report.pdf

D. Mini-Case Study IV: Developing the Viet Nam National Single Window

a. Introduction

Viet Nam is a member of the ten-nation ASEAN. Since at least the mid-2000s, ASEAN and its Member States have been working towards the development of a regional Single Window as an element of their overall economic integration strategy. In 2005, the ASEAN Member States signed the ASW Agreement[82] and in 2006, they entered into the ASW Protocol.[83]

b. Master Plan and Roadmap

In order to fulfill its obligations under the *ASW Agreement*, Viet Nam had worked diligently to develop the organizational framework to effectively engage in preparations for developing the Viet Nam Single Window (VNSW). Under a Prime Minister's Decree issued in 2008, a National Steering Committee was established, composed of senior government officials, to oversee the VNSW development and implementation efforts. The National Steering Committee appointed a Standing Bureau under the General Department of Customs of Viet Nam for implementation of the Viet Nam NSW project. A Legal Working Group has been set up within the Standing Bureau to oversee the legal implementation of VNSW.

Viet Nam also requested assistance from the ASEAN Secretariat[84] in developing the VNSW, including for a legal analysis that focused on identifying potential gaps in the domestic legal framework for the full implementation of the electronic SW and its cross-border interoperability with the ASEAN SW. The formal work on this project began in 2009 with the implementation of an extensive Fact Finding program that sought to assess all aspects of Viet Nam's trade and regulatory systems and operations that would be related to the VNSW, including all Ministries involved in the import, export and transit of goods as well as port and border operations.

The results of this Fact Finding effort were presented at a VNSW National Workshop in June 2009 in Ha Noi. This Workshop reviewed a proposed VNSW Master Plan that covered 14 different areas, including legal issues.[85] The proposed VNSW Master Plan Template included a "High-Level Roadmap to Establish a Viet Nam National Single Window" that included key tasks and subtasks correlated with the VNSW Master Plan Template. This Roadmap included specific activities, assigned responsibilities, and the proposed timelines within which the work would be completed. The following Box III.1 shows the major tasks related to the legal aspects of the VNSW Roadmap.

BOX III.1. Viet Nam single window roadmap – legal tasks

Legal Activities

Steering Committee must provide an explicit mandate for the Legal Working Group (LWG) and its work, including:

- Establish requirements (or regulations) that Ministries provide representatives to the LWG;

[82] Agreement to Establish and Implement the ASEAN Single Window, Kuala Lumpur, (9 December 2005).

[83] Protocol to Establish and Implement the ASEAN Single Window, (20 December 2006); see also, Vientiane Action Programme, signed at Vientiane Lao PDR (29 November 2004).

[84] Assistance and support for this effort was provided by the USAID under its ASEAN Single Window Project, which is part of the ADVANCE Program managed by Nathan Associates Inc

[85] They included: 1. Concept of Operations; 2.Data Standardization; 3. Data Model; 4. Data Flow Diagrams; 5. User and Functional Requirements; 6. Technology Infrastructure; 7. Technical Reference Model; 8. Cost- Benefit analysis; 9. Project Administration and Long Term Strategy; 10. Configuration Management; 11. Project Implementation and Transition Plan; 12. Training Plan; 13. Communications Plan; 14. Legal Issues.

BOX III.1. (cont.)

- Require that Ministries provide all legal and other relevant information that will be both (1) needed by the LWG to complete its work and (2) that is related to the development of a lawfully operating VNSW;
- Provide the mandate for the LWG to complete its work within the context of the Vision, Mission and Objectives of the VNSW Master Plan;
- Provide the mandate for the LWG to work with the TWG and other groups and sub-groups, Ministries, and Departments to draft regulations (e.g., on information security, the pilot project, and other relevant areas where technology intersects with legal issues) for the VNSW;
- Include provision for LWG participation in outreach activities;
- Provide timetable for the LWG to complete its work.

Develop LWG Workplan

Review existing regulations (including all laws and decrees) that may impact the operation of the VNSW in order to identify possible impediments to operating the VNSW in either the electronic or paperless environments, including:

- Review any international agreements to which Viet Nam is a Contracting Party (e.g., IMO, CMI, IATA, WHO, etc.) that have requirements for "documents" that must be "in writing" and/or "signed" that do not expressly permit that these may be electronic and that may be related to the VNSW;
- Review other Ministry laws, regulations, and/or decrees that may require adjustment in order to fully analyze the needs for domestic legal harmonization to facilitate the operation of the VNSW;
- Review ASEAN Single Window Agreement and Protocol, ASW Steering Committee workplan, ASW LWG workplan, and other relevant ASEAN agreements to ensure the VNSW will be able to lawfully integrate with the ASEAN Single Window;
- Conduct preliminary analysis to determine how all of these laws and decrees will affect the creation and operation of the VN Single Window;
- Review and analyze information above and prepare appropriate recommendations for inclusion in the LWG workplan;
- Study the possible benefits to Viet Nam and the VNSW of ratifying the UN Electronic Communications Convention and consider the application of Article 20 of the Convention to other International Agreements to which VN is a Contracting Party;
- Develop specific recommendations for the Steering Committee to create new laws (possibly including legislation, decrees and/or regulations) and/or to modify existing laws, decrees, and/or regulations to provide the necessary legal infrastructure for the lawful operation of the VNSW;
- Work with all groups involved in the development and management of the VNSW throughout the project on issues that intersect law, technology, and policy;
- Draft revise/new laws/regulations to provide necessary legal infrastructure for operation of the VNSW and joining the ASW;
- Participate actively, involving Viet Nam's lawyers and legal experts, in the ASW Legal Working Group and ratify the ASW Legal Framework Agreement when finalized;
- Participate in outreach activities.

c. Legal Gap Analysis

Refinement of the legal tasks contained in the Roadmap continued during 2009 along with discussions concerning the undertaking of a formal legal gap analysis for the VNSW. In early 2010, a formal request for proposals was issued for a *Legal Analysis for Implementation of Viet Nam National Single Window*.[86] This request for proposals described the legal topics that would be included in the legal gap analysis. These legal issues are included in Box III.2.

The request for proposals also described the research methodology that the legal consultants should use in conducting this legal gap analysis. Given Viet Nam's legal national approach, the consultant was expected to use a standard legal research methodology typical of a highlevel research effort. Thus, the methodology for this research and report was structured as follows:

- Primary legal sources should represent the research focus. These would include enacted legislation, statutes and laws, decrees and executive orders, circulars and the like, etc., having the force of national law, formally adopted and promulgated regulations and rulings, judicial and administrative decisions, etc.

BOX III.2. Research issues for the VNSW legal gap analysis

Electronic transactions legal issues, including:

- Legal issues related to identification and authentication in an electronic transactions environment;
- Legal requirements for electronic documents and messages;
- The need for development of legislation or other regulations dealing with electronic transactions for the SW;
- Policies (executive acts, instructions or documents of similar nature), legislative enactments, administrative rulings, regulations and governmental decrees, circulars and the like that would formally establish the SW in national laws;
- Development of a service level arrangement for the operation of the SW;
- Laws and regulations on data protection and information security;
- Regulatory and/or legal requirements for accessing and sharing information and data between and among government agencies;
- Legal requirements, if any, in national law and regulations, on confidentiality and privacy;
- Laws and regulations relating to data accuracy and integrity for the SW;
- Liability issues related to operations of the SW and, its eventual cross-border transactions;
- Regulatory/legal requirements for data retention and electronic archiving issues;
- Dispute settlement considerations;
- Intellectual property rights and data base ownership issues;
- Cross-border recognition (mutual recognition) of electronic signatures and, where appropriate, certification authorities;
- Legal issues related to jurisdiction in cross-border transactions;
- The use of electronic evidence in, for example, judicial and enforcement proceedings;
- Competition law issues (including treaties and conventions, and GATT requirements that may be applicable to Viet Nam) related to SW;
- An analysis of how international legal standards have been (or have not been) incorporated into Viet Nam's legal framework for its SW;
- Other legal related issues, deemed necessary, to complete the task.

[86] This RFP was issued by the USAID ADVANCE Program, managed by Nathan Associates, that assists the ASEAN Secretariat and the ASEAN Member-States in the development of the ASEAN Single Window as well as the NSWs of various Member- States. The terms of references for the legal gap analysis was developed through the ASW Working Group on Legal and Regulatory Affairs as a template to be used by ASEAN Member States at the national level.

- Secondary legal sources (e.g., legislative history, ministry, administrative and executive reports), should also be reviewed and included to provide background and interpretations of the primary legal materials.
- References to other legal materials (e.g., law review articles, conference reports, international commentary) may also be included if relevant to the development of the VNSW and related electronic commerce legal framework developments in national law.

d. Legal Gap Analysis Process and Final Report

The contract for the VNSW Legal Gap Analysis was awarded in the late Spring 2010. And intensive 3-day Kick-Off Meeting was conducted in Ha Noi during June 2010. Participants included Viet Nam Customs, the ASEAN Secretariat, USAID representatives from the ADVANCE Program, the ASW Legal Working Group Legal Advisor,[87] and the consultants[88] who had been awarded the contract. The meeting participants engaged in an extensive review of the legal issues to be addressed in the gap analysis, the process involved in gathering all of the inputs required for the research and analysis, and the timetable for the Interim and Final Reports.

Following the kick-off meeting, consultants spent considerable time reviewing and analysing all of the legal materials that were identified for the legal gap analysis. An interim report was prepared and presented to the VNSW Legal Working Group. After additional research and discussions, including information collected from other ministries and private sector, an extensive draft Final Report was prepared and presented to a larger public and private sector audience. Following review by, and feedback from, the VNSW Legal Working Group, the final version of the *Legal Analysis for Implementation of Viet Nam National Single Window* was submitted in May 2011. The consultants noted in the introduction that,

> *"In performing this gap analysis, we note that Viet Nam has made strong progress in the modernization of its laws for electronic transactions. The law in Viet Nam is substantially harmonized with the UNCITRAL Model Laws of Electronic Commerce and Electronic Signatures, and also the United Nations Convention on the Use of Electronic Communications in International Contracts. What remains to be done is for the Viet Nam government to promulgate legislation that will develop, establish, implement and operate the VNSW, which will be fully authorized and empowered to perform all its functions as a National Single Window. This report provides recommendations to the Viet Nam government on the requirements of such legislation to cover any gaps in the current legal environment."*

Viet Nam has continued to implement the findings of the Report, where necessary, as it completes the work to create a fully operational SW that will be interoperable, both technically and legally, with the ASEAN Single Window and with Single Window facilities outside the region.

FURTHER READING

"Legal Analysis for Implementation of Viet Nam National Single Window", Nathan Associates inc. USAID ASEAN Single Window Project, which is part of the ADVANCE Program supported by USAID and the U.S. Department of State (2011). Available at http://advanceiqc.com/uploads/vnsw-legal-gap-analysis-final.pdf

[87] The ASW Legal Advisor provided extensive background on the ASW LWG work, international Single Window developments, and overall guidance regarding the legal issues that are essential to the development of a legal framework for a SW and its cross-border interoperability.
[88] The winning bid was submitted by a Singaporean law firm, in partnership with a Vietnamese law firm.

Glossary

Alternative dispute resolution	Dispute resolution processes such as negotiation, mediation and arbitration, which occur out of court.
Authentication	The process of verifying the identity of a party to electronic transactions against its credentials.
Authorization	The act of granting permission for someone or something to conduct an action (e.g., in the SW environment).
Certification authority	A trusted third party who has the authority to issue digital certificates vouching for the identity of the holder of the digital certificate.
Cross-border recognition	The legal recognition of, e.g., data, processes, methods and standards across national borders.
Data authenticity	The correct attribution of the origin of data.
Data integrity	A concept relating to the validity of data and its representational faithfulness to the true state of the object that the data represents.
Data privacy	A concept covering the various issues and topics concerning, in general, limitations on access to and use of data in order to protect its confidentiality.
Data retention	A concept covering the policies, legislative instruments and procedures for recording and storing data for legal and other purposes.
Digital certificate	An electronic document connecting a party's identity to a public key. The certificate includes various identification information related to the party.
Digital signature	Electronic signatures providing a higher level of security, often using public key infrastructure technology.
Electronic signature	Data in electronic form in, affixed to or logically associated with, a data message, which may be used to identify the signatory in relation to the data message and to indicate the signatory's intention in respect of the information contained in the data message
E-commerce / Electronic commerce	The trade in products or services over electronic systems and networks, including the Internet.
E-Government	The electronic interaction between the government and its citizens. If related to electronic customs procedures, it is called E-customs.

Electronic archiving	The electronic retention and upkeep of data records often in accordance with data retention norms.
Electronic data interchange	Structured transmission and exchange of data between organizations and individuals by electronic means
End-User License Agreements	An agreement between the licensor and the licensee establishing the licensee's rights to use the licensed software.
Functional equivalence	Identity of legal treatment provided, when certain conditions are met, to paper-based documents and electronic communications.
Identification	The release of electronic credentials to an entity providing evidence of its identity
Non-discrimination	The equal legal treatment of paper-based documents and electronic communications.
Non-repudiation	A service that provides proof of the integrity and origin of a data message or an authentication measure that can be asserted to be genuine with high assurance.
Paperless trade	The conduct of trade using electronic data and documents rather than paper documents.
Phytosanitary measures	Measures preventing the spread of pests of plants and plant products.
Private key	In public-key cryptography, the private key is a key (string of characters) used for decryption and signing which is private to the users.
Public key	In public-key cryptography, the public key (string of characters) is used for encryption and verifying the authenticity of electronic signatures and it is known to the public.
Public key infrastructure (PKI)	A specific system of digital certificates, certificate servers and Certification Authorities based on public key cryptography techologies.
Public-Private Partnerships	A public service or private business venture which is managed and funded through a partnership of the government and at least one private sector company.
Single window / National single window	A facility that allows parties involved in trade and transport to lodge standardized information and documents with a single entry point to fulfill all import, expert, and transitrelated regulatory requirements. If information is electronic, then individual data elements should only be submitted once.
Service Level Agreements	A contract between the service provider and the customer which formally defines the service and the related details.

Bibliography

Asian Development Bank, "Singapore's TradeNet System", Philippines. Accessed at: http://www2.adb.org/Projects/TradeFacilitation/publications-tradenet.asp on 13 March 2012.

Asia-Pacific Economic Cooperation, "Evolution of Singapore's Single Window." Single Window Working Group Capacity Building Workshop 4: Singapore. Available at: http://www.wcoomd.org/files/6.SW_Files/SW%20Initiatives/APEC/APEC%20-%20Singapore%20Evolution%20of%20Single%20Window%20-%20April%202009.pdf

Chan Wah Teck, J., "Legal issues in e-commerce and electronic contracting: the Singapore Position."Asean Law Association. (2009). Available at: http://www.aseanlawassociation.org/docs/w5_sing.pdf

Chong, K. W., "Legal and Regulatory Aspects of International Single Window Implementation: The ASEAN Experience", Global Trade and Customs Journal, 4, pp. 185–193 (Kluwer Law International, 2009).

Field, R., "ASEAN Single Window: Introduction to Service Level (and Related) Agreements."Working Paper, Sixth Meeting of the ASW Working Group on Legal & Regulatory Matters, Da Lat, Viet Nam (2009).

International Convention on the Simplification and Harmonization of Customs Procedures (Revised Kyoto Convention). Available at: http://www.wcoomd.org/Kyoto_New/Content/content.html

Koh Tat Sen, J., "Blazing new trails", Crimsonlogic Pte. (2009) Available at: http://www.unescap.org/tid/projects/tfforum_exhibit_crimsonlogic.pdf

Luddy, W. J., "International Single Window Development", UNCITRAL Colloquium on Electronic Commerce, (New York, 2011). Available at: http://www.uncitral.org/pdf/english/colloquia/EC / Luddy.pdf

_____, "ASEAN Single Window: The Intersection of Law and Technology" (2008). Available at: http://pdf.usaid.gov/pdf_docs/PNADM816.pdf

McLinden, Gerard, Enrique Fanta, David Widdowson and Tom Doyle, "Border Management Modernization", World Bank (2010).

Sathasivam, K., "The Single Electronic Window –Singapore's TradeNet –Scope of Services and Pricing Model", CrimsonLogic Pte., Singapore (2009). Available at: http://www.carecprogram.org/ru/uploads/events/2009/Single-Window-Workshop/Day2-TradeNet.pdf

Schermer, B., "Legal Issues of Single Window Facilities for International Trade," UNCITRAL Congress – Modern Law for Global Commerce (July 2007).

Singapore Customs, "In SYNC online newsletter", Issue 14 (2011). Available at: http://www.customs.gov.sg/insync/Issue14/article_5.html

Thomson, L., "Legal Infrastructure Issues in Privacy, Information Security and Information Sharing Practical Steps for the Development a Secure Trade Data System". Presented at the 6th Meeting of the ASW Working Group on Legal & Regulatory Matters, Da Lat, Viet Nam (2009).

_____ (Editor), "Data Breach and Encryption Handbook", American Bar Association, 2011.

UN/CEFACT Recommendation 33 – Recommendation and Guidelines on establishing a Single Window to Enhance the Efficient Exchange of Information Between Trade and Government (ECE/TRADE/352, July 2005) United Nations publication, Sales No. 05.II.E.9. The paper is available at http://www.unece.org/fileadmin/DAM/cefact/recommendations/rec33/rec33_trd352e.pdf

UN/CEFACT Recommendation No. 35 – Establishing a Legal Framework for the International Trade Single Window (2010), available at http://www.unece.org/cefact/recommendations/rec_index.html

UNCITRAL Model Law on Electronic Commerce, Article 5. Legal recognition of data messages. (1996). Available at: http://www.uncitral.org/uncitral/en/uncitral_texts/electronic_commerce/1996Model.html

UNCITRAL Secretariat, "Promoting Confidence in Electronic Commerce: Legal Issues on International Use of Electronic Authentication and Signature Methods", United Nations Publication Sales No. E.09.V.4.(Vienna, 2009). Available at: http://www.uncitral.org/uncitral/en/uncitral_texts/electronic_commerce.html

UNCITRAL, UN Convention on the Use of Electronic Communications in International Contracts, Available at: http://www.uncitral.org/pdf/english/texts/electcom/06-57452_Ebook.pdf

UNECE, ECE/TRADE/371 "A Roadmap Towards Paperless Trade," (2006). Available at: http://www.unece.org/cefact/publica/ece_trd_371e.pdf

UNNExT, "Case of Korea's National Paperless Trade Platform, Towards a Single Window Trading Environment" Brief No. 3. (2010). Available at: http://www.unescap.org/unnext/pub/brief3.pdf

_____, "Best Practice in Single Window Implementation: Case of Singapore's TradeNet", Towards a Single Window Trading Environment, Brief No. 02 (2010). Available at: http://www.unescap.org/unnext/pub/brief2.pdf

WCO Secretariat, WCO Compendium of Authorized Economic Operator AEO Programmes (July 2010). Available at: http://www.wcoomd.org/files/1.%20Public%20files/PDFandDocuments/research/aeo_compendium1.pdf

Winn, J., "The Emperor´s New Clothes: The Shocking Truth About Digital Signatures and Internet Commerce", Idaho L. Review, 37, 353 (2001).