Part 2:

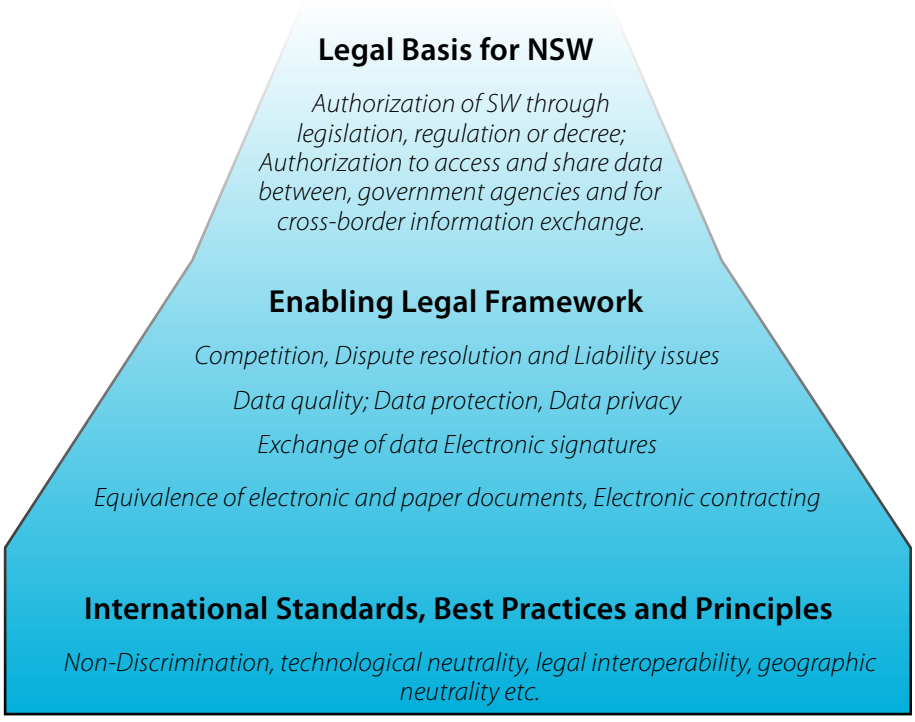
Essential Legal Elements for the Implementation of a National Single Window

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;