Cloud single window: legal implications of a new model of cross-border single window

Luciano Pugliatti

Abstract

In his paper, 'Weaknesses in the supply chain' published in this Journal,[1] David Hesketh discussed the problems and threats for customs authorities that arise from lack of visibility in the supply chain of what is really being carried inside cargo containers. According to Hesketh, this is due to the fact that the information supplied to Customs and other authorities in all jurisdictions involved derives from different sources and, for various reasons, it is altered, summarised or manipulated to the extent that it is no longer a true representation of the goods being carried. This has serious implications not only for the collection of proper duties but also for the identification of counterfeit, dangerous or prohibited goods and for supply chain security.

Hesketh posits that the solution lies in a re-think of how the supply chain is being managed by capturing information about the cargo as close as possible to the source, that is, from the consignor, and in ensuring that information does not change when it is made available to border authorities downstream. To make this happen, Hesketh proposed building 'a web-based, seamless electronic "data pipeline" linking the seller/consignor and the buyer/consignee and interested economic operators in-between' with customs authorities.[2]

In this paper, I have suggested a potential system architecture that governments could implement in order to facilitate and take advantage of this data pipeline (the *Pipeline*) and I have explored the legal issues involved. The architecture proposed would require a new international convention but it would address the issue of integrity of the supply chain as well as provide for greater trade facilitation. It is also a model that, by taking a different angle, reduces the complexity of the legal issues involved.

1. Introduction

The supply chain is the end-to-end movement of materials and goods from origin to final destination during which the goods may undergo a number of transformations, are subject to a number of commercial transactions and are transported by different means of conveyancing.

Several economic operators (EOs) are involved in the supply chain. Along the way these different operators acquire title to the goods or materials and responsibility in relation to those goods with regard to regulatory obligations within their jurisdiction.

In a globalised economy, the modern supply chain may span several countries and, therefore, the EOs responsible at any one time for selling, packaging, handling, shipping, storing and, ultimately, importing the goods are subject to the laws and regulations of different jurisdictions.

In order to comply with their regulatory obligations the fundamental requirement for the EOs is to provide truthful and accurate information about the goods for which they are responsible to the relevant authorities in their jurisdiction.

The supply chain has been described as 'traditionally characterised by a forward flow of materials and a backward flow of information'.[3] In a supply chain that involves cross-border movements of goods, Customs and other border agencies are recipients of information except that, ideally, they need the information to flow 'forward' ahead of the physical movement of the goods rather than 'backward' (that is, once the movement has taken place).

Prior knowledge of what kind of goods are to be expected at the border has become an imperative in recent years for two main reasons.

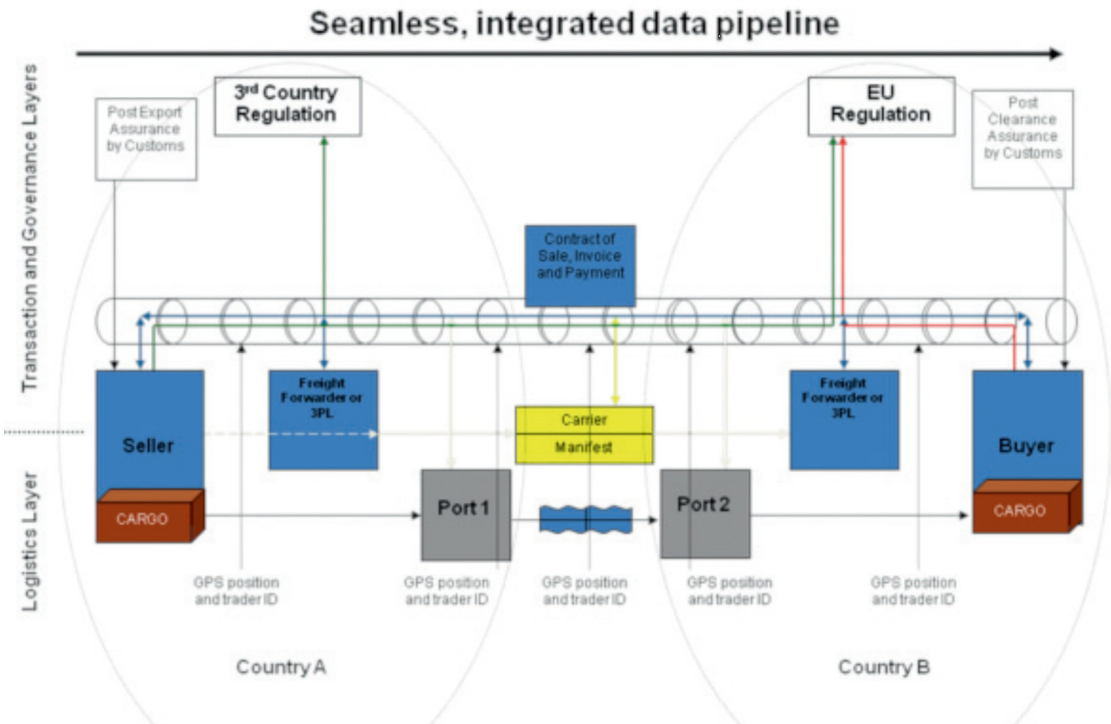
Firstly, there is a growing responsibility put upon border agencies and Customs in particular to promote trade facilitation by speeding up and simplifying clearance procedures at the border.

Secondly, there is a need to screen goods ahead of arrival in order to detect potential security risks. In the wake of the 9/11 events, there has been a growing concern that the supply chain is exposed to terrorist threats or that it could be used to fuel terrorist activities.

Therefore, it is imperative that Customs and other border agencies should receive information about the cargo that they are expecting that is accurate and, ideally, they should have access to this information as soon as it becomes available in the supply chain.

For this to happen, Hesketh advocated the creation of the *Pipeline* described in the following figure (Figure 1) and argued that a new international convention will be required.

Figure 1: Supply chain data Pipeline



Source: David Hesketh 2010.

The key concept of the *Pipeline* is that EOs should find it advantageous to place commercial and logistics information about a consignment in the Pipeline for the purpose of transacting their business and that Customs (and other relevant border agencies), across jurisdictions, should leverage that information in order to discharge the regulatory obligations and carry out risk assessments without requiring that this information should be re-submitted by different parties.

The fundamental assumption is therefore that regulatory authorities should use the actual information which is used in the contract of sale of the goods and in the fulfilment of the transaction rather than a traditional separate declaration.

In this paper, I conceptualise a system architecture that governments could implement so that Customs and other border agencies can 'piggyback' onto the Pipeline and I explore what the legal issues might be around implementing such a thing. I also consider whether the recent trend towards 'cloud computing' would present opportunities to facilitate the implementation of the *Pipeline* principle and, if so, what legal issue that would present.

2. National single window as the gateway for the Pipeline

In the model that I propose, there would be a shared, supranational facility that provides a service to the national authorities of the participating states. I have called this facility ***Cloud Single Window*** (CSW).

The technologies and methodologies for a collaborative e-commerce platform are already proven by well-established examples of logistics networks, such as Tradegate[4] in Australia or TradeXchange[5] in Singapore, that allow the exchange of electronic messages between commercial and logistics operators as well as providing for the interchange, at national level, of certain messages with Customs and other government authorities.

Similarly, the concept of exchanging commercial data using agreed standards, such as Rosettanet,[6] to carry out international transactions between commercial operators – using private networks, VPNs (Virtual Private Networks) or other forms of secure communications – is also well established.

The CSW model is aimed at leveraging these facilities already implemented in the commercial sector, which I have referred to collectively as the *Pipeline*, in order to create a concept of regional or international single window which is aimed at ensuring supply chain integrity and visibility by serving as more than just a routing network for electronic messages between customs authorities.

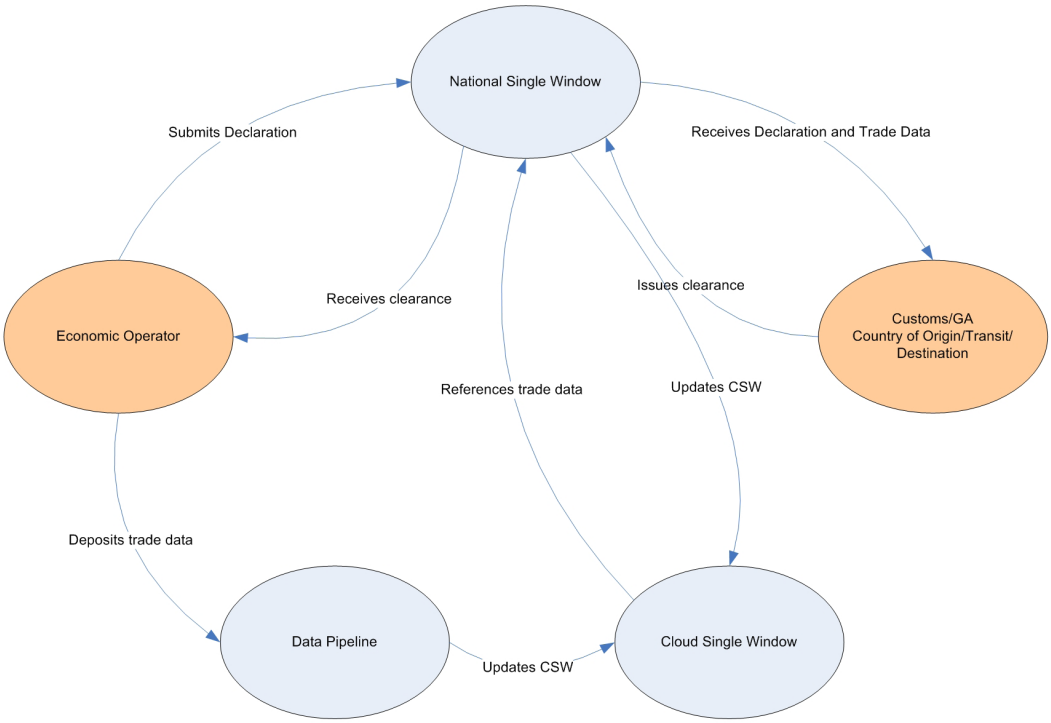
The CSW would be the governments' interface with the commercial *Pipeline* and each participating state would link into it (and, by proxy, the *Pipeline*) through their *national single window* (NSW) acting as the gateway.

At its basic level, the CSW would therefore be a platform for the interconnection of national single windows. This concept, often referred to as 'Regional Single Window' or 'Cross-Border Single Window' or 'International Single Window', is not new and is actually encouraged by the United Nations Centre for Trade Facilitation and Electronic Business (UN/CEFACT) and the World Customs Organization (WCO). However, there are no examples of one having been implemented and, therefore, there is no accepted international model yet. In any event, the prevailing models of an international single window contemplated so far do not envisage leveraging a commercial data pipeline, and they are simply predicated on an exchange of data between customs authorities. Such an example is the Association of Southeast Asian Nations (ASEAN) Single Window which is probably the only regional single window in the process of implementation, albeit in pilot mode. The model currently being contemplated predicates a Government-to-Government (G2G) exchange of information between NSWs which is independent of the Business-to-Business (B2B) pipeline and, therefore, falls short of delivering real-time visibility on the supply chain.[7]

3. Proposed new model of supranational single window

Essentially, the CSW would be a wide area network (WAN) the stakeholders of which are the government authorities of each country involved in the supply chain (that is, Customs and other border agencies). These stakeholders would interact with the CSW through their NSWs and the CSW would be seamlessly interconnected with the *Pipeline*, which could be any combination of the commercially operated facilities mentioned above, as illustrated in the following high level conceptual model, Figure 2.

Figure 2: Conceptual model of Cloud Single Window (CSW)



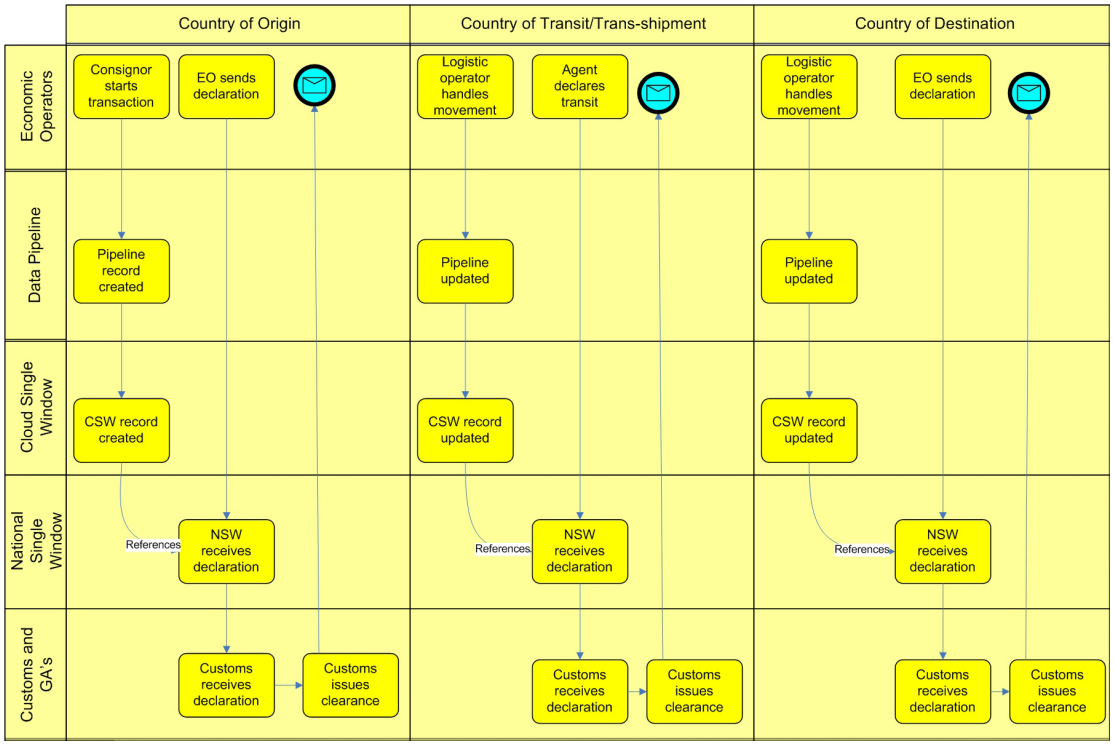
Source: Pugliatti 2010.

The CSW would act as the repository of commercial transaction data from the start through to the end of a transaction involving the shipment of goods across borders.

Conceptually, the *Pipeline* and the CSW could be the same network but this would present an increased level of complexity from legal and operational points of view due to having to accommodate the requirements of both private and public sector within the same environment and across borders.

A high level conceptual representation of the CSW process flow is illustrated in Figure 3 below.

Figure 3: Model of Cloud Single Window (CSW) operation



Source: Pugliatti 2010.

The starting point for the CSW is from the *Pipeline* where the EO deposits details of the goods at the start of a commercial transaction. The CSW would open an electronic 'pipeline record' for that consignment using a Unique Consignment Reference Number (UCRN) as the identifier.

As the consignment progresses along the supply chain, other EOs will take responsibility for it and will be obliged to report a movement relating to it (for example, loading, departure, arrival, discharge) or submit a declaration (for example, export, transit, import) to border agencies within their jurisdiction. In current practice, each party that is responsible for reporting or declaring the consignment sends a message to the authorities containing a description of goods which may originate from their internal systems or may have been re-created through manual processes. This may take the form of a notice of arrival/departure, discharge/load list, tally manifest, cargo/freight manifest, customs declaration as well as any number of commercial supporting documents that national legislation may require.

In the CSW model, each EO may fulfil the above requirements by lodging a message with their NSW which simply identifies the movement or transaction being reported by making reference, by means of a UCRN, to the consignment/s which relate to that transaction recorded in the CSW.

If any changes are necessary to the description of goods, quantities, weight, etc. once the consignment data has been lodged into the CSW, the operator would send a message referring to the original record with any modifications. The change would be stored in the CSW as part of the consignment's history.

For the above to happen, one key legal aspect is that an electronic message carrying legal value (such as a customs declaration) must carry the same legal weight even if it does not contain the full data payload but, instead, it points at another document stored within a third-party domain (the CSW).

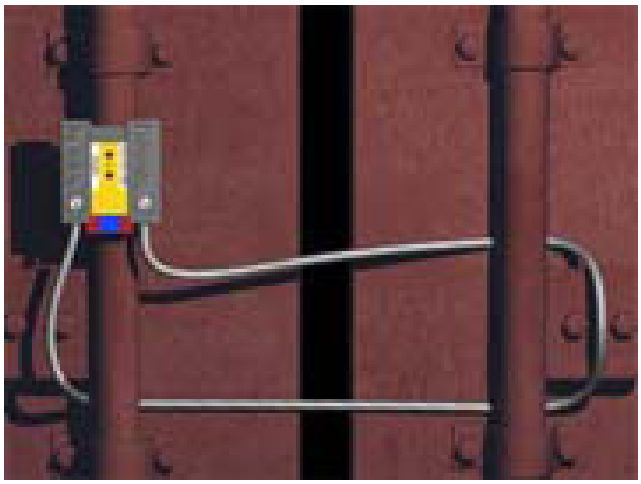
The key factor is that Customs and other agencies always have access to the original data. In the CSW model, Customs and other authorised border agencies will have access to the data for any consignments destined for their jurisdiction as soon as the original commercial transaction record is placed in the *Pipeline* and the CSW. The CSW could issue an alert electronically to the relevant authorities downstream in the supply chain as soon as a 'pipeline record' is created and every time that record is updated with tracking information.

In his paper, Hesketh advocated the use of RFID and GPS technology for granular tracking of goods at unit, pallet, consignment and container level.[8]

Following 9/11 there have been a number of projects experimenting with these technologies aimed at providing real time visibility on the location of goods, especially when stuffed inside containers, as well as attempting to guarantee that the contents of the container have not been tampered with since the original stuffing thus still corresponding to the description carried by the various transport documents.

One such technology is the 'electronic seal'. There have been various prototype electronic seals developed and tested, such as the one shown in the picture below (Figure 4), though most of them fail to live up to their manufacturers' promises of total tamper prevention.

Figure 4: Tamper detecting electronic seal



Source: Universeal UK Limited 2003.

Every time the seal is read at checkpoints along the supply chain (for example, vanning, de-vanning, gate-in, gate-out, loading, discharging, re-positioning, etc.) the operators' systems could relay that information to the *Pipeline*/CSW so that real-time tracking of the cargo position can be made available to all the CSW stakeholders.

There are vast logistic and commercial difficulties in establishing the use of electronic seals across the entire supply chain, at least until the cost of packaging the technology into a device comes down to the level where re-usability is not required. However, as and when these issues are overcome and the cost of technology becomes viable, electronic seals coupled with other technologies like GPS, may prove to play a vital role in ensuring the integrity of the supply chain.

Advantages of the CSW model

What are the advantages of the CSW model as against the traditional one of a regional single window simply acting as a routing service for e-documents (the 'flow through' model)?

Firstly, in the traditional model, once the data has been routed to an intended recipient, it is no longer visible by all other government stakeholders in the supply chain. In the CSW model the complete history of the consignment including, possibly, any movements registered via RFID or GPS devices, would be visible in real-time to all stakeholders in all relevant jurisdictions. This means that, given the necessary safeguards about privacy and confidentiality, it could provide a shared platform for risk assessment by customs authorities in all participating countries, giving them valuable access to advance information as well as traffic pattern analysis.

Secondly, the CSW does not predicate that an exporter's declarations 'flow through' to Customs in the importing country, thus raising a host of legal issues to do with liability for false declarations and others. The CSW model relies on parties in the supply chain electing to accept responsibility for the data lodged at origin at the start of a commercial transaction. If they have no objections to that data being used, they can confidently use it as the basis for their declaration. If, on the other hand, they have objections, they would have the opportunity to submit an alternative data set in which case, potentially, an alarm trigger may be raised with the relevant authorities to investigate the reason for the discrepancy. The principle of 'commercial advantage', gained from a higher level of differentiated treatment by the border authorities, should dictate that most operators will prefer to avoid unnecessary delays by electing to use the CSW data where there is no good reason on their part not to do so.

The CSW model is philosophically in line with the recommendations made by the WCO in its *Resolution on the Role of Customs in the 21st Century*:

> The new requirement is to create, in partnership between the various stakeholders of the public and the private sectors, a global Customs network in support of the international trading system. The vision of this network implies the creation of an international 'e-Customs' network that will ensure seamless, real-time and paperless flows of information and connectivity.[9]

Both the *Pipeline* and the CSW would require a technical and logical infrastructure that sits outside the jurisdiction of each country in the supply chain. Whilst in the case of the *Pipeline* this would be subject to a commercial agreement between the EOs, in the case of the CSW the infrastructure and the service would need to be shared by different national authorities.

4. Legal implications of the Cloud Single Window (CSW)

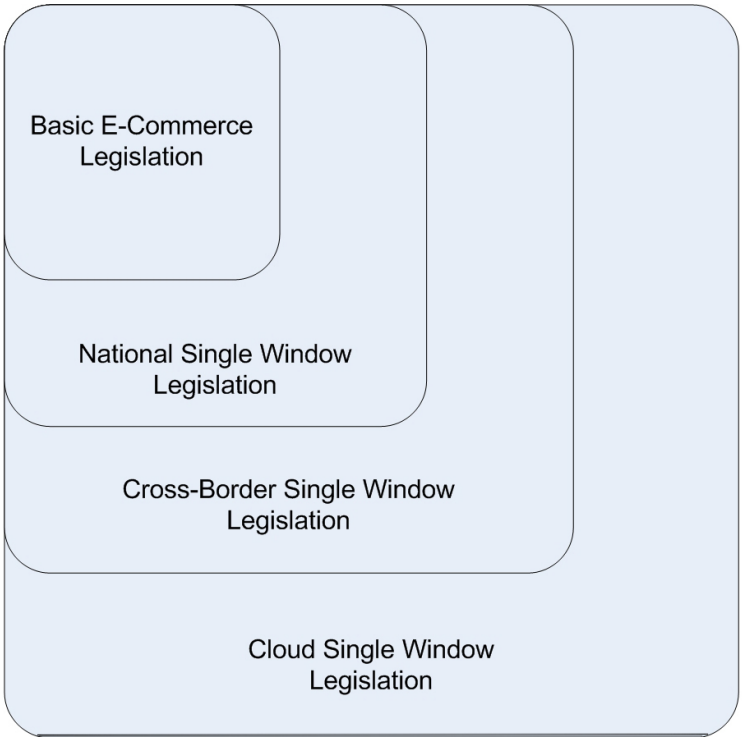
In examining the legal implications of a CSW I have tried to posit measures that require a minimum of mandatory legislation over and above existing frameworks.

CSW relies on certain basic assumptions about the existence of a legal framework that enables information to be received into it, form part of a declaration and be retained over time in the CSW environment. The information would primarily be the contents of a commercial transaction with accurate descriptions of goods, value, quantity, weight, marks, origin, destination and other relevant details.

Therefore, the legal framework for the CSW must be based, incrementally, on the foundations of existing e-commerce legal frameworks that cover the supply chain.

The relationship between these levels of legislation can be described by the diagram below, Figure 5.

Figure 5: Legal framework for CSW



Source: Pugliatti 2010.

National e-commerce legislation

At the fundamental level of any single window legislation is the ability to exchange information that carries legal value between an EO and Customs or any other government agency within its own jurisdiction.

A large number of countries have already enacted basic legislation to allow electronic transactions to take place covering both Business-to-Government (B2G) and Government-to-Business (G2B) transactions.

Much of this legislation is based on the United Nations Commission on International Trade Law's (UNCITRAL) *Model Law on Electronic Commerce* which provides a framework for the key principles, that is,

- allowing electronic commercial transactions to carry legal status in place of paper documents – this is known as the principle of 'non discrimination'
- retention of data stored electronically in place of physical archives
- integrity of electronic messages
- attribution of messages
- acknowledgement of receipt of messages between parties.

National single window (NSW) legislation

Above the basic e-commerce level, there must be a legal framework for operating an electronic NSW.

A checklist of issues to be considered when implementing a national or international single window is provided by *UN/CEFACT Recommendation No. 35* though some of them are the basic principles of e-commerce listed above.

- Data protection
  The principle of data protection and the right to privacy or confidentiality of the data supplied to the NSW should be enshrined in national legislation.

- Identification, authentication and authorisation
  Identification of the originator or recipient of a message, authentication of his [*sic*] credentials and authorisation to carry out certain transactions are the means to ensure the integrity of the data being submitted and an appropriate level of access to the various facilities of a National Single Window thus also addressing the issue of where liability lies.

  UN/CEFACT Recommendation 35 recognises that 'there are no worldwide legal, procedural and technical standards in this area at the present time'[10] and this is probably also due to the fact that there are many different technological ways of addressing these issues. For example, digital signatures or digital certificates can be used to provide authorised access or authentication of messages. To use such facilities a Public Key Infrastructure (PKI) is required which is, basically, a service managed by a 'trusted third party' (also known as 'certificate authority') that provides authentication of digital message exchanges based on a digital key uniquely associated with a user of which the PKI authority is the trusted custodian.

  There are, however, a number of technical variations and, indeed, there is a school of thought that digital signatures are redundant in an environment where an accredited user is immediately recognised through their login and password credentials and that the 'signature' is implicitly assumed through the interchange agreement in existence between the parties.

- Data quality
  The quality of the data (assuming that modern computers, networks and data transport protocols can be trusted not to distort or lose data in transmission) is only as good as what is supplied by the originator. Therefore this issue comes down, again, to identification and authorisation of the originator of the message and to the legal framework that governs receipt, acceptance and legal status of that transaction.

  In a single window context, the first step of identification is to allow only approved registered users to have access to different facilities on offer according to their role within the supply chain.

- Liability issues
  These are issues that may arise from the misuse of information or from supplying incomplete, incorrect or false information. The liability arising from such issues is closely tied to the provisions governing identification, etc., and data quality as discussed above and the respective responsibilities of the parties involved.

- Authority to access and share data between government agencies
  In the context of a typical NSW, the model would be such that all the data required by all the agencies to give clearance is submitted to a single point, through a single channel and, preferably, as a single message. This means that even if the data is 'sliced and diced' so that each agency receives only the data that it requires, it would still exist, before and/or after that is done, in a domain to which all agencies, potentially, have access. Conversely, in a model where one agency operates the NSW facility on behalf of other agencies, that agency would have access to information which pertains to other agencies.

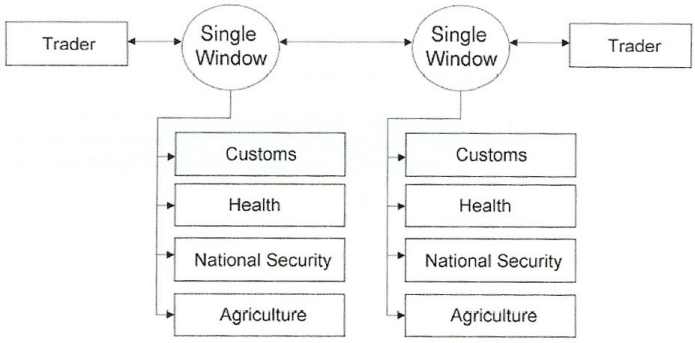
It is therefore necessary to write into law the ability to share information between agencies and for a single submission to be valid as a declaration to all the agencies. The law should confine the sharing of information to certain agencies for the purposes of border control and exclude any entity that may have a commercial interest in the information (for example, an airport authority).

Cross border legislation

The third level is the legal framework for exchanging information between government agencies across borders.

Schermer used the simple diagram below (Figure 6) to describe what an international single window would do.[11]

Figure 6: Model of international single window



Source: Schermer 2007, p. 3.

In this model, the concept of an international single window comes down to an exchange of certain documents once these have been submitted to, validated and generally processed by an NSW.

Therefore, the advice that follows is that 'on an international level, bi-lateral or multi-lateral agreements often need to be established to govern the operations of each single window and that take into account a variety of legal issues that may arise to ensure "legal interoperability" between these single windows'.[12] Similarly, UN/CEFACT *Recommendation 35* recommends that in international agreements there should be 'mutual recognition of electronic documents and data messages that may be exchanged between single window facilities'. The general conclusion is that, in order to provide a legal framework for an international single window, there should be harmonisation of national laws, something that is clearly going to be challenging to achieve in the short to medium term given the disparate level of national law in many countries.

The key principle underlying the models envisaged by UNCITRAL, UN/CEFACT and ASEAN seems to be that an international single window is a facility for routing e-documents – the integrity of which is guaranteed by national legislation – between NSWs that will accept the validity of those documents on the grounds of mutual recognition of each other's national legal frameworks.

However, in the 'flow-through' model where the declaration (and documents) data is exchanged Customs-to-Customs, the issue of recognising a message sent by Country A to Country B as valid and carrying legal weight in the receiving jurisdiction has proved very difficult. ASEAN, for example, thought it presented 'significant difficulties for the efficient and effective enforcement of laws of Country B'.[13]

The CSW model attempts to circumvent these legal difficulties at the same time as addressing the issue of real-time visibility of the supply chain by predicating a different functional architecture that requires a simpler legal framework.

In the conceptual model of CSW, the fundamental principle is that a message containing trade data is delivered to the CSW from the commercial *Pipeline* and, therefore, mutual recognition of customs declarations is not necessary.

However, it will be necessary to create an international convention (the **'CSW Convention'**) whereby all the parties would agree to the rules governing the CSW in respect of data protection, privacy and identification of the information being shared.

The CSW Convention would have to address the following issues.

Ownership

First and foremost is the issue of ownership in the sense of being responsible for the infrastructure, for the service it provides to its users, for protecting the confidentiality of the data and for administering the data within the agreed rules of interchange.

The obvious consideration is that, as it is a service to national authorities that have signed up to it, the managing entity should be a body that represents, equally, the interests of all these stakeholders.

The European Union (EU) provides a model for such cooperation as it already operates a number of systems in an integrated architecture for its members (for example, TARIC [Integrated Tariff of the European Communities], NCTS [New Customs Transit System]) and others – most significantly SEAP (Single Electronic Access Point) – that are under development as part of its eCustoms vision.[14] However, this is made possible by the body of legislation that supports the Customs Union, primarily the *Modernized Customs Code*.[15]

In the absence of such a framework, a CSW open to all countries that wish to take advantage of it and that are not necessarily members of a union could be operated by a body that represents a membership with common goals.

One option would be a 'members owned' cooperative association, along the lines of SWIFT for the banking sector, which would have to accept the 'CSW Convention' as the basis for its constitution. However, this organisation would not have a legal personality that would enable it to dictate that sovereign states should, as may be necessary from time to time, change their national laws and, as in the case of SWIFT which is incorporated under the laws of Belgium, it would have to be subject to the law of wherever it is based which may not be acceptable to some of its members.

The other alternative would be for an established international organisation to take the operation of the CSW under its wing. The United Nations Conference on Trade and Development (UNCTAD) may be a candidate but, for the reasons below, the WCO would seem to be more appropriate.

The WCO has the legal personality to draft and enable a convention which can put obligations on its parties at a national level. The WCO can also acquire property, institute legal proceedings, hold different currencies and transfer funds,[16] all of which would be necessary conditions to enable it to operate a facility such as the CSW as well as charging a fee for the service, if necessary. The WCO could therefore be the custodian of the 'CSW Convention', open for voluntary accession, which would embody the Service Level Agreement (SLA) between the WCO and the parties to the convention as well as the interchange agreement between the CSW and the commercial organisation responsible for managing the *Pipeline*.

The WCO could also provide the premises for the CSW at their headquarters which, under the *Customs Co-operation Convention 1952*,[17] is considered to be an inviolable supranational location thus resolving the issue of parties having to come to terms with the service being operated under the national law of another member as well as being free from liabilities, taxes, prosecutions, etc. arising from any national law.[18]

In fact, there is already a precedent for such an arrangement as the WCO has been running for some years a system called CEN (Customs Enforcement Network) which offers Members the facility to exchange data relating to seizures and trans-national crime. Furthermore, the *Johannesburg Convention* makes provisions for a 'secure central automated information system' managed at the WCO's Headquarters.[19]

Capture of original data from the consignor

The key feature of the *Pipeline* concept is to capture data regarding a consignment from a reliable source (the real shipper) as close as possible to the start of the supply chain. This data would be voluntarily placed into the *Pipeline* by the EO using the data that constitutes the contract of sale.

Mandating in law that the real shipper should be obliged to do so would seem to be a step too far. Ultimately, EOs should be convinced that there is a commercial advantage in complying with this requirement which will be reflected in the treatment of their consignment along the entire supply chain.

However, a measure of integrity may be catered for by national Authorised Economic Operator (AEO) schemes which would confer each EO an appropriate degree of trust. This degree of trust could be reflected in a 'hallmark' affixed to each transaction and carried through to the CSW which could be used by customs authorities down the supply chain to assess the degree of risk that the data carries in terms of accuracy.

The way in which the data is assembled prior to submission could be subjected to the normal audits for verifying AEO compliance which could include inspection of the AEO's computer systems to ascertain whether their data originates straight from electronic contract of sale documents.

Of course, whilst the above may ensure the integrity of the information down the supply chain, it cannot guarantee that the information is accurate in the first place if the shipper is engaged in some form of illegal activity. This is something that can only be addressed by customs authorities through their intelligence and risk management programs.

Use of UCRN, authorisation and identification

The CSW would rely on each consignment being uniquely identified throughout its life cycle. This can be done through the use of a UCRN. The use of a UCRN has been advocated by the WCO by means of a recommendation[20] and there is therefore a substantial obligation on Members to enforce its use through national legislation.

The important issue to note is that, in the CSW, an EO down the supply chain can choose to submit a declaration by making reference to the original data using the UCRN as the key identifier.

There are technical issues concerning the use of a UCRN. However, from a legal perspective, it is immaterial who issues the UCRN but its use and the rules governing its generation would have to be written in national law and the 'CSW Convention' should provide for harmonisation of these rules.

Security can be enforced by issuing a private key to the original operator who lodged the consignment at the start of the supply chain and that key would be uniquely associated with the UCRN for that transaction. It would then be the responsibility of the original operator to communicate the UCRN and its associated private key to their trading partners down the line. In this way, only the EOs legitimately involved in that transaction will have access to the original data and Customs, in any of the jurisdictions down the supply chain, will know that they are authorised to do so by their trading partners.

In this scenario, alongside issuing the UCRN, the service provider of the CSW could also be the ideal vehicle for providing the PKI services to all its members so that a common security standard can be adopted. Indeed, the use of PKI is advocated by the WCO in the *SAFE Framework of Standards*[21] and it is catered for in Data Model 3.[22]

Liability

Perhaps the most important issue is that of liability for the information supplied, that is, whether this can be used as evidence in any particular jurisdiction and what to do to enforce any liabilities given that it may not have been originated by a party in that jurisdiction.

In the CSW model, liability for a declaration would rest with the EO that has submitted a declaration message to their NSW making reference to the data supplied via the *Pipeline*. The basis for accepting an e-document that makes reference to another e-document is already covered by the UNCITRAL Model Law as a fundamental principle of e-commerce. Therefore, liability and use as evidence fall within the national jurisdiction of the receiving authority.

The legal instrument that carries liability and that can be used as evidence is the 'declaration message' submitted to an NSW which contains a reference to the data and, unlike the 'flow-through' model, no electronic document is being passed from one government agency to another across borders thus mutual recognition of electronic customs declarations is not necessary.

Eventually, it may be desirable to make the originator of the data liable for inaccurate or false descriptions. This would require a high degree of harmonisation of national laws and an international agreement to allow prosecutions in another jurisdiction and, undoubtedly, the legal issues involved in this respect are likely to be complex.

Standard to be used for messages

This is probably the easiest issue to address because all that is required is that the CSW Convention's members agree to submit or retrieve data to/from the CSW in an agreed format. It is immaterial what format each NSW enforces on its users nationally and, indeed, an NSW, similarly to services such as Tradegate's MessageXchange,[23] should allow economic operators to submit declarations and other messages using formats that are in wide international usage, for example, EDIFACT, UNeDocs, and XML.

From the perspective of the data set, again, if the WCO were to take an active role in CSW it would become easier to stipulate the use of the WCO Data Model 3.

Confidentiality

The issue of confidentiality of the data retained in the CSW is probably the most controversial. As Luddy states, 'Ensuring confidentiality, integrity, availability and privacy of information and data are fundamental to protecting the information assets of government and private sector participants'.[24]

It is understandable that what ostensibly looks like one big database containing all the trade data related to the participating countries' – albeit conceivably only for the lifetime of the transaction – would raise the concern that it could, firstly, be mis-used by other members to gain some advantage and, secondly, could be the target of hacking.

On the danger of unauthorised access by hackers all that one can say is that, obviously, the danger does exist but, as in other security-conscious applications like banking, the benefits of doing it outweigh the danger. The CSW would have to adopt the most stringent security measures available to the ICT industry to prevent such attacks and in this respect it is no different from any public service that is, to different degrees, exposed to the outside world through the internet. Such measures could include the use of proxies to shield access to the main database/s, 128-bit encryption on all communications via the internet, storage of data in encrypted format requiring a private key to decode it, spread of data over separate locations, and so on.

On the question of whether authorised members trust each other to only use the data for legitimate purposes, protection of each member's interests in this respect would have to be incorporated in the CSW Convention along the lines of the national legislation that governs the sharing of information between government agencies within a country. Therefore, the basis for this mutual trust could be mutual recognition agreements between members.

National law may prevent countries to share information across borders. Indeed, concerns about sharing information may account for the poor take-up by states of the *Johannesburg Convention*. However, these concerns may be alleviated by the fact that, in the CSW concept, what is being shared is not operational customs data but data voluntarily submitted by the private sector. Therefore, it is the private sector that should be comfortable with the provisions on confidentiality and data protection that would be embodied in the CSW Convention and these concerns should be addressed in the SLA between the CSW operator and the *Pipeline* operator/s.

5. Running the Cloud Single Window in a 'cloud' environment

Throughout this document I have referred to the 'cloud' in relation to the proposed model of a supranational single window. In this respect, I have used the term loosely to signify that the CSW does not run in any specific jurisdiction and that it provides a service to users across national boundaries.

In technical terms, however, the prevailing modern meaning of 'cloud' is a service provided by a supplier that delivers to end users the information and functionality they require (whether through web screens or data packet exchanges with their back-office systems) by using an infrastructure which does not reside with the end users and could, indeed, be reliant on data centres or computer facilities in more than one location anywhere in the world.

The reason for exploring the feasibility of operating the CSW as a 'cloud' service is that this is now a topical subject. The recent WCO IT Conference held in Seattle in May 2011 was boldly entitled '*Cloud Computing – A New Era for Customs*' and its thrust was that 'cloud' technology is now mature enough to be able to offer Customs the opportunity to run collaborative systems such as single window in a potentially massively scalable environment with substantial gains in efficiency and savings in cost.

In the CSW model where a supranational organisation like the WCO would take ownership of providing the service, one could conceive the traditional model where a large computer is installed at their headquarters with all the necessary telecommunication devices to enable external access by users over the internet. In this case, the data, the software and the hardware would reside in one specific place. There is nothing wrong with this model except that the service would have to be kept operational 24/7, provisions would have to be made for backup and disaster recovery and, most importantly, a very high degree of scalability would have to be built into this infrastructure as the data repository will very quickly get larger and larger and the volume of transactions bigger and bigger as the service grows. This would require a hugely sophisticated ICT support capability on the part of the provider and the cost of running such an operation would be substantial.

The advantages of the 'cloud' model are that the client/s do not have to maintain and support the infrastructure and the systems; they are guaranteed virtually limitless scalability and do not have to deal with a variety of contracts or SLAs with different technology suppliers.

This is where an arrangement whereby CSW is operated on a 'cloud' platform would, in theory, present several benefits. However, a number of legal issues would need to be resolved in a model where an organisation, such as the WCO, would be the client 'owning' the CSW and providing a service to its members but where this service is provided, via a contract with a 'cloud' provider.

A report by an Expert Group to the European Commission (EC) identified the great potential for

cloud applications and, indeed, its main recommendation was that the EC should stimulate research and development and address the regulatory aspects and issues of standards in order to encourage its development and expansion. However, the report acknowledged that there are still gaps both on the technology side and on 'the legalistic side of cloud systems'. [25]

For the purpose of this paper, I will set aside various technical issues (for example, broadband speeds, and scalability of telecom infrastructure) and assume that sufficient progress, as has always been the case with technology, will be made to address these issues. I will also set aside whether a 'cloud' service is any more secure than a privately-owned service and, suffice to say, for various technical reasons it would probably provide a higher level of security against unauthorised access though no-one can ever give a 100% guarantee.

As 'cloud' is a relatively new concept it follows that there are no established models to address the key issues, and most literature that I have researched simply enumerates the various issues that need to be considered or that are problematic without actually offering a solution. For example, the Expert Group's report to the EC simply states 'new legislative models have to be initiated, and/or new means to handle legislative constraints'.[26]

In any 'cloud' contract there would have to be, of course, all the normal provisions in terms of performance, business continuity, disaster recovery and quality of service which would have to be embodied in an SLA for which many established models exist in the context of outsourced contracts. For example, in a lot of the commentary about the 'cloud', much is made of the perils of losing all the data through a catastrophic disaster. From a technical perspective, this is a potential danger that applies equally to in-house computers as to outsourcing. Therefore, a client would demand guarantees to be written into a 'cloud' contract in the same way as any outsourced contract.

Similarly, the same issues in terms of protection of trade secrets that arise from sensitive data being placed in the hands of a commercial provider apply for the 'cloud' and, also, these would have to be covered by non-disclosure clauses in the contract.

In the CSW context, the main issue is not only that critical and highly confidential data would not be within the client's physical control but also that they do not necessarily know where it is. In a 'cloud' contract, the concept of the location where a service is being performed is indeterminate and, indeed, the service breaks down into different levels, that is, data storage, data processing (the systems), data transport (telecommunications) and end-user presentation. All of the above components of the service could utilise locations and infrastructure spread over different countries. Indeed a piece of data, before it is presented to a user, could have been manipulated in and have traversed several jurisdictions.

This begs the question as to which jurisdiction applies in terms of data protection, confidentiality, intellectual property rights (IPR) infringements as well as, of course, contractual liabilities. If the client demands certain standards about data protection, the 'cloud' provider may not be able to offer guarantees that the data will not be handled, at some point during the processing, storing or backing up, in a country where the data protection laws are not adequate and, therefore, the data would be at risk if, during the processing, it were to 'stick' or leave a trace on computers located in that country.

To a certain extent, however, the above problems already exist when the internet is used as the transport medium for any transaction as the end user has no control over the journey or the handling of the transaction's payload. In the case of the CSW, the main sticking point would appear to be where the data is actually stored. This would have to be in a location or more than one location with which the client is comfortable in terms of local data protection legislation. This means that whatever piece of infrastructure is operating at any given location that may hold or process the client's data, is under the jurisdiction of national law in that country and could be subjected to a search warrant or seizure by national authorities in that country, even if the contract with the 'cloud' provider falls under another jurisdiction.

At first glance, it would therefore seem unlikely that an organisation such as the WCO or the CSW's stakeholders would contemplate operating the CSW as a pure 'cloud' given the likely concerns about privacy and mis-use of information. However, there are alternative solutions, for example:

- A 'private cloud', that is, a 'cloud' infrastructure operated solely for an organisation. Some providers are willing to create a 'point of presence' in a known location in a specific country (hence under a known jurisdiction) if the scope of the contract justifies it.
- A 'community cloud', similar to the above except that it is operated for the benefit of more than one organisation.
- A 'hybrid cloud', that is, a combination of any of the above with the public 'cloud' depending on the level of security that different types of interaction require.

6. Conclusions

In this paper I have outlined a suggested model and architecture for a supranational single window which could be implemented by governments alongside the commercial *Pipeline* in order to improve supply chain visibility. The model leverages the existence (present or future) of NSWs and differs from current envisaged models of a regional or international single window in that it is not based on a bilateral exchange of electronic documents but it predicates the existence of a real-time repository of shared data.

The advantages of this model in relation to traditionally envisaged models are that it would provide real-time visibility over the cargo along the entire supply chain whilst guaranteeing the integrity of the data available to Customs and other border agencies.

This model can be implemented using currently available internet technology and infrastructure and, potentially, it could be implemented using an infrastructure and facilities operated in a 'cloud' environment.

From a legal perspective, whilst there are important issues to be resolved, there are few real impediments, at least for those countries that have already implemented the fundamentals of e-commerce, as most can be achieved by leveraging existing legal frameworks.

At the foundation, should lay a solid framework for e-commerce implementable using the *UNCITRAL Model Law* as a template and, indeed, this has already been done in a number of countries. The basic e-commerce legislation should, however, be extended to allow an NSW to share information between agencies with the necessary protections in terms of confidentiality and privacy. Again, in a number of countries, this has already been done.

However, for the CSW, it is also necessary to have a legal framework to allow sharing of information (*not e-documents*), with the necessary confidentiality and data protection measures, between agencies across borders. Whilst there is no existing example of such a framework, the WCO has laid the foundations in the *Nairobi Convention* and the *Johannesburg Convention* and is actively encouraging the creation of an e-Customs network. In this respect, in the CSW model, things are simplified by the fact that no data is being passed from government to government as the information is derived from data voluntarily supplied by EOs.

It would, however, be necessary to draft a new convention to allow the operation of the CSW and this convention may incorporate a number of the provisions already existent in the *Nairobi* and *Johannesburg Conventions* with regard to confidentiality and data protection.

It would also be necessary to establish an organisation to operate the CSW on behalf of all the governments and this should be an organisation that represents the interests of all the stakeholders. I have suggested that the WCO would be ideally placed for such a role as it has a legal personality that

allows it to draft a convention and, if necessary, require that members should make changes to national law. Another advantage of the WCO taking on such a role would be that the CSW would be operated under a supranational jurisdiction which is not subject to the laws of any one country. This would remove one of the most often heard objections to any collaborative arrangement.

However, the CSW may be too big an undertaking in terms of technology infrastructure and operational commitment for an organisation such as the WCO. I therefore considered what the alternatives could be in terms of operating such a model and what legal issues they raise.

One traditional model is outsourcing where the client would enter into a contract with a service provider. This is a well-established model with many examples of government agencies outsourcing their data collection and processing to commercial operators. This kind of arrangement could take different flavours such as operating an off-site facility or one on the client's premises or a mixture of both.

The other model that is emerging is the 'cloud' where the client outsources the service to an operator that uses an infrastructure that takes advantage of the distributed nature of the internet in order to offer virtually unlimited scalability and computing power as well as economies of scale. The difficulties that would arise in this model for the CSW would be in the fact that, in a pure 'cloud' model, the client has no knowledge of where the data is kept and, therefore, whether it is safe from intrusion or juridical interference.

Unfortunately, the 'cloud' is still a relatively new concept for which there is no established legal framework. To quote the Research Centre on IT and Law (CRID): 'Currently Cloud computing seems closer to fog than cloud and it might constitute a real danger for the users and data subjects whoever they are…'.[27]

Therefore, it would seem unlikely that, given their already high concerns in terms of data protection, stakeholders would consent to such a highly security-conscious operation as CSW being operated in a pure 'cloud' environment, at least in the immediate future. There are, however, alternatives – all essentially variations on outsourcing – such as a 'private cloud', a 'community cloud' or a 'hybrid cloud' where the supplier may provide localised, identifiable locations for all or some of the services to be provided through the 'cloud'.

In conclusion, the CSW is a different model from the ones normally envisaged for an international single window but it is a model that would address the issue of integrity of the supply chain as well as trade facilitation. It is also a model that, by taking a different angle, reduces the complexity of the legal issues involved. Technology has moved to the point where there are no impediments to its implementation. What remains is the willingness to embrace it and to make it work! Much work would remain to be done to reach the necessary agreements but, in this paper, I have attempted to outline a vision and a potential way forward.

Endnotes

1 Hesketh, D 2010, 'Weaknesses in the supply chain: Who packed the box?', *World Customs Journal*, vol. 4, no. 2, pp. 3-20.

2 Hesketh 2010, p. 3.

3 Beamon, BM 1998, 'Supply chain design and analysis: models and methods', *International Journal of Production Economics*, vol. 55, no. 3, pp. 281-94.

4 Tradegate, www.tradegate.org.au/.

5 TradeXchange®, www.tradexchange.gov.sg/tradexchange/default.portal.

6 Rosettanet, www.rosettanet.org/.

7 USAID/ADVANCE 2011, *Development of the technical architecture for the ASEAN single window pilot project*, April, p. 14, www.nathaninc.com/sites/default/files/Pub%20PDFs/DELIV%2007%20-%20ASW%20Pilot%20Project%20Component%201%20-%20Overall%20Physical%20and%20Logical%20Architecture%20v2.00.pdf.

8 Hesketh 2010, p. 18.

9 World Customs Organization(WCO) 2008, *Resolution of the Customs Co-operation Council on the Role of Customs in the 21st Century*, June.

10 United Nations Centre for Trade Facilitation and Electronic Business (UN/CEFACT) 2009, *Recommendation 35, Establishing a Legal Framework for International Trade Single Window*, Draft Version 9.0, UN/CEFACT.

11 Schermer, BW 2007, *Legal issues of single window facilities for international trade*, UN/ECE/CEFACT Legal Group, p. 3, www.uncitral.org/pdf/english/congress/Schermer.pdf.

12 Schermer 2007, p. 4.

13 Kah-Wei Chong 2011, *Legal and regulatory aspects of international single window implementation: the ASEAN experience*, 27/38, February, UNCITRAL Colloquium on Electronic Commerce, New York.

14 European Commission 2004, 'Draft eCustoms vision statement and multi-annual strategic plan', TAXUD/477/2004, Rev. 3, October.

15 *Official Journal of the European Union* 2008, Regulation (EC) No. 450/2008 of the European Parliament and of the Council of 23 April 2008 laying down the Community Customs Code (Modernised Customs Code), June.

16 WCO, *Convention Establishing a Customs Cooperation Council*, 1952, Annex, Article II, Section 2.

17 WCO, *Convention Establishing a Customs Cooperation Council*, 1952, Annex, Article II, Section 4.

18 WCO, *Convention Establishing a Customs Cooperation Council*, 1952, Annex, Article II, Sections 3, 5, and 8.

19 WCO 2003, *International Convention on Mutual Administrative Assistance in Customs Matters (Johannesburg Convention)*, Article 31.

20 WCO 2004, *Recommendation of the World Customs Organization concerning a unique consignment reference (UCR) for customs purposes*, June.

21 WCO 2007, SAFE Framework of Standards, para. 6.7.

22 WCO Data Model Ver. 3, WCO ID: 104, Authentication.

23 Tradegate, MessageXchange, www.tradegate.org.au/products/messagexchange/.

24 Luddy, WJ 2011, *International single window development*, February, UNCITRAL Colloquium on Electronic Commerce, New York.

25 Schubert, L 2010, *Expert Group Report: the future of cloud computing*, European Commission, p. 3.

26 Schubert 2010, p. 33.

27 CRID (Research Centre on IT and Law) 2010, 'Cloud computing and its implications on data protection', Draft Discussion Paper, March, Council of Europe, Strasbourg, p. 4, www.coe.int/cybercrime.

Luciano Pugliatti

Luciano Pugliatti (Luc) is an independent ICT consultant with over 15 years' experience of delivering solutions for customs and revenue administrations. He has designed and implemented innovative ICT systems aimed at revenue enhancement and modernisation of customs and tax administrations in many countries in Africa, Eastern Europe, the Caribbean and South East Asia. He has carried out diagnostic missions for the World Bank and has acted as ICT Adviser to Vietnam Customs and, currently, to the Lao Ministry of Industry and Commerce.

Prior to working in the public sector, Luc owned and operated a software company that specialised in shipping and trade logistics systems with an emphasis on electronic data interchange (EDI) solutions. His clients included some of the major shipping agents and lines in the United Kingdom and Europe.