TAX AND COMMERCE OECD

REPORT BY THE TECHNOLOGY TECHNICAL ADVISORY GROUP (TAG)

December 2000

REPORT BY THE TECHNOLOGY TECHNICAL ADVISORY GROUP (TAG)

TABLE OF CONTENTS

REPORT BY THE TECHNOLOGY TECHNICAL ADVISORY GROUP (TAG)

EXECUTIVE SUMMARY

Introduction

1. The Technology TAG has undertaken a range of work with the Consumption Tax and Professional Data Assessment (PDA) TAGs and the Working Party No. 9 Sub-Group on Electronic Commerce ("WP9 Sub-group") in examining the technological implications of the various collection models considered for collecting consumption taxes on cross-border electronic commerce transactions and the reliability of indicators systems and trails for audit purposes. This work is brought together in this report to summarise the Technology TAG's conclusions at this point in time. Where appropriate, each section sets forth suggestions of where continued work is required. As a further mandate, the TAG looks to continuing work in resolving the extant issues presented by the various technologies, most of which are quickly evolving as is all the technology underlying electronic commerce.

2. Annexes to this paper provide a range of supporting detail to this executive summary.

Scope

3. The mandate of the Technology TAG has developed into that of a responsive expert group providing contextual information regarding the applicability of technological solutions to issues of audit, tracking and collection. Beyond applicability, the Technology TAG also provided estimates of reliability and evaluated solutions based on the practicability of implementation. Implementation issues included factors such as cost, efficacy and commercial reasonableness.

4. Generally speaking the tax collection issues which we were asked to address implicitly contain four fundamental assumptions:

- First, the electronic transaction type which is the most susceptible to tax avoidance and requires a tax collection solution is that of "virtual products[1]" sold from businesses to consumers.

1. Virtual products as used in this paper includes all goods or services which are or can be provided completely over electronic media. This term covers goods and services which may not be subject to tax or which may be the subject of disagreement or inconsistent national and sub-national classification. It is not the intent of this paper to address those issues.

- Second, the primary means by which consumers will access the Internet for the purchase of "virtual products" will be via computers or interactive TVs and, over time, through mobile devices[2] but most virtual products are not suited to download by current mobile phones.[3]
- Third, although this paper deals primarily with VAT and similar consumption taxes, any system which is designed must necessarily take into consideration alternative systems such as the Sales / Use tax system in the United States.
- Lastly, the dominant issue for consumption taxes is cross-border transactions.[4]

Collection model options

5. While the paper considers the four primary models that have been advanced for the collection of consumption taxes on cross-border e-commerce transactions, we would stress that we do not see these models as mutually exclusive from a technological perspective. It is important to ensure that any first steps towards implementation of a collection model is consistent with the development of a longer term solution. This is a necessary step to minimise business compliance costs as well as the ease of administration by revenue authorities.

6. We also advocate the implementation of the ultimately agreed model on a smaller scale such as the sale of virtual products from businesses to consumers as a viable short term starting point. Clear signals from government in relation to the preferred long-term solution would also facilitate businesses working with government without the distraction of dealing with short-term proposals.

7. We also highlight the fact that end-to-end virtual transactions are currently a very small part of e-commerce and a fractional non factor in commerce overall. We deal primarily with these issues in this paper because of the context of the questions put to us. We also recognise the potential for significant growth in this area and that the complexity of the inherent issues coupled with the pace of technological innovation and maturing of business models will require more intense study to develop appropriate solutions in advance of significant growth in this area.

Relevant technologies

8. Successfully implementing a viable consumption tax collection model will require harnessing of the same technologies that businesses are adopting for their electronic commerce initiatives. Inherent in this is the need to link collection mechanisms with the underlying business models to maximise the return on the necessary investment for both business and government.

---

2. Less than a computer but more than a phone. Most will have touch screens and small hard drives in a form factor along the lines of today's larger Personal Data Assistants (Palm, Psion, Pocket PCs).

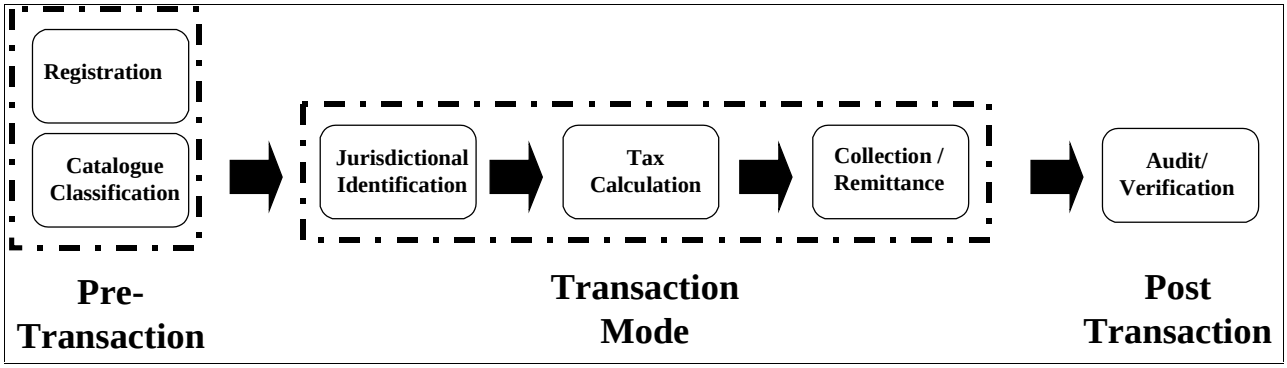
3. Any solution proposed for collection of consumption taxes must however be flexible enough to deal with mobile access. While virtual products are not downloadable to mobile phones a variety of virtual services are already available through wireless portals. Massive growth in the numbers of wireless device users accessing the Internet over the next few years is being forecast by most observers (for example, see IDC.com).

4. With an understanding that certain jurisdictions such as the United States have complex sub-national sales and use tax systems which pose similar issues.

Shared technological elements

9. Before examining the collection models that have been proposed for our review by the WP9 Sub-group, there are a number of shared technological elements common to many of the tax collection/administration models which the Technology TAG has investigated. From a technological perspective, we have found it useful to consider the models from the perspective of the broad activities or modules represented in Figure 1.

Figure 1. Shared technological elements



10. The primary differences between the proposed collection models are then limited to how this logical model would be physically implemented (for example, who would have responsibilities for different activities).

Jurisdictional verification

11. The module which has presented the greatest challenges for the Technology TAG is the jurisdictional identification module. Common to all models, the challenge is to provide merchants with a mechanism which, *inter alia*, allows the jurisdiction of their consumer to be verified (see Annex III). *This information is essential if the Ottawa Framework Condition to the effect that taxation should be in the jurisdiction of the consumer is to be implemented.*

12. Annex IV provides a "Technology Primer for Identity of Parties and Classification" which discusses the potential technologies and their strengths / limitations. The primary findings of the Technology TAG in relation to the identification of a consumer's jurisdiction are:

1) The simplest form of jurisdictional identification is to accept a **consumer self-declaration** of their jurisdiction. The financial incentive for a consumer to incorrectly declare their jurisdiction in order to avoid consumption taxes means that this solution, while technologically simple to implement, has major limitations from a government perspective, giving rise to increased scope for revenue risk. Some form of verification of the consumer's self-declaration will be necessary if a degree of reliability acceptable to revenue authorities is to be obtained.

2) In conjunction with **payment system providers**, an examination was undertaken of the potential for using credit card numbers, credit card billing addresses or other information inherent to credit cards to verify a consumer's jurisdiction. Annex V details the results of this examination. While we are continuing the dialogue with the credit card companies, the Technology TAG's conclusion is that the credit card business processes do not provide a workable verification methodology. In addition, the directions of the payment system providers' business models mean that the current verification limitations will only become greater over time. It is therefore unlikely that revenue authorities' jurisdictional verification needs will be met through these avenues unless a (currently non-apparent) strong business rationale can be identified to provide a suitable return for the payment system providers.

3) Internet Protocol (IP) addresses offer potential in that they are an essential part of every access point to the Internet. **IP traces** have some limitations (such as single worldwide access points for AOL users and corporate aggregators, use of anonymisers, plans for IPv4 to be replaced with IPv6[5] and potential for spoofing) such that the costs of implementation may not be worthwhile.[6] Given today's technology, the limited improvement in location technology offered by IP traces appears to be the best available, but there is a significant reluctance on the part of business to undertake implementation of such systems because of concerns of the lack of commercial necessity, limited utility, almost assured obsolescence of IPv4 traceware in the near to medium term, costs of implementation and potential for disruption of service in cases of unclear results. Lastly, while inquiries have uncovered that IPv6 does not currently include a predictable geographic component, further work needs to be done to better understand the potential for jurisdictional identification. IPv6 tracing technology will need to be monitored as it develops. Governments need to be aware that the pseudo-geographic link between IP number and jurisdiction can potentially be significantly strengthened. However this will become harder and costlier to accomplish once full, rather than trial, deployment of IPv6 begins. Research on this must be a priority as IPv6 deployment is expected within the next two years.

4) Technology-based options utilising **digital certificates**, alone or in conjunction with trusted third parties, could offer genuine potential in the medium to long term. This requires an uptake by consumers and a change in existing business-to-consumer models. However commercial deployments are now underway and businesses are beginning to invest in consumer solutions. More detailed examination of this potential, and how best governments might support and utilise it, is an important field of further work.

5) The Technology TAG understand and agree on the need to find a practical short term solution to meet the needs of government without negatively impacting the ability of business to engage in online commerce or imposing unreasonable burdens of compliance. It is possible that **viable short-term solutions** may not be technological solutions (*e.g.* the use of a merchant's internal databases). Progressing viable short-term solutions should be one of the first items of work for the Technology TAG once it reconvenes.

---

5. Internet Protocol numbers are the Internet equivalent of a phone number or address. The current protocol is Internet Protocol Version 4 (IPv4) which defines an Internet address a unique number consisting of 4 parts separated by dots, *e.g.* 165.113.245.2

6. The experience of US-based cryptography exporters in using IP numbers to verify purchasers' country in order to meet Bureau of Export Exchange requirements is of an estimated 60 to 70% matching of IP address with the self-declaration was achieved. Note that a mismatch was not the only check as companies also checked against a denied parties' access list which increased the reliability for the agencies involved.

6) Any solution must also encompass the increasing consumer sensitivity and industry responsiveness to concerns about **privacy and data protection**. Many commercial systems are being designed on a more need to know and permission marketing based information architecture. There is thus a significant reluctance on the part of business to collect more information than that needed for commercial purposes. This trend is also impacting the future developments in payment systems.

13. We suggest that the whole area of jurisdictional verification needs further work. To be done properly, this work may eventually require a dedicated team of experts. We stress the need to complete further basic research before settling on any collection model or method that requires technological deployment. The policy and practice are symbiotic and need to be developed concurrently. Resolving policy independently of understanding the required technology may lead to policy that can't be practically implemented.

14. These limitations also lead the Technology TAG to caution re moves away from place of consumption as the principle for imposing consumption taxes on digital products. Moves by the WP9 Sub-group towards using place of residence as the basis for taxation may limit the options for technological verification in the future (see Annex VI). With the major exception of digital certificates, technology may be as or more likely to be able to determine a consumer's location (*i.e.* place of consumption) in the longer term rather than their place of residence. We therefore advocate that flexibility should remain in the longer term defining of "place of consumption".

The collection models

15. The Technology TAG's conclusions in relation to each of the four primary consumption tax collection models identified in further detail in Annex II are set out below. As discussed above, we examined the collection model from the perspective of a logical model detailing the broad activities or modules required for a successful implementation. We have also commented below on the "Simplified Interim Approach" advocated by the Consumption Tax TAG.

16. While a version of the Tax at Source and Transfer / Trusted Third Party models[7] is the Technology TAG's favoured model of those initially considered, we would advocate that future discussions concentrate on determining how each of the above six modules could best be implemented to achieve the goal of a successful consumption tax collection model. The most efficient and effective long term solution must successfully address all six of these elements.

The self-assessment option *See Annex VII*

17. Self-assessment is seen as a viable option for business-to-business transactions. No technology issues have been identified.

18. While there is little cost to a pure self assessment deployment (additional inquiry field in web pages) there are significant government concerns in relation to the reliability of the resultant data. The technology costs and the low likelihood of a successful commercial deployment or a reliable verification

7. It should be noted that all Tax at Source & Transfer, the Trusted Third Party and the Hybrid models discussed in this paper have the same underlying logical model. The differences stem from how the model is implemented and responsibilities for the various functions are shared / split between the business, trusted third parties and revenue authorities involved in the tax calculation and collection process.

system result in a recommendation that this option is the least practicable for business-to-consumer transactions from a technology perspective. The view of the Technology TAG is that a Self-Assessment model that government agencies would find reliable creates almost insurmountable problems to implement from a technology standpoint. Limitations in current registration options, identity verification issues and difficulties in verifying many small payments from many sources combine to make a model which can not be robustly implemented with the currently available technology.

The registration option *See Annex VIII*

19. The major technology issues posed by this model are the identification of the consumption tax status of the customer; verifying the jurisdiction of the consumer, identifying non-resident suppliers and developing systems capable of compliance once those factors are established.[8]

20. Technology appears to be capable of providing solutions to the first two issues in the medium term. The resolution of these issues is also required for the collection models discusses below. While solutions are advanced for the identification of non-resident suppliers, it is unlikely that the taxation net will ever be completely robust.

21. The Technology TAG sees the imposition of significant compliance costs on non-resident suppliers, especially those making supplies in multiple jurisdictions or making nominal supplies, as an important drawback of this model. The provision of easily accessible information on the Web or an enhanced system to provide a goods classification and calculation routine on the Web is advanced as a possible technological solution to improve the implementation of this model. These solutions are also important components of the following collection models. In looking at simplification of compliance and sharing of burdens suggestions were made relating to globalising applications, simplifying rates and calculation and having burdens of compliance equitably shared where appropriate.[9]

The tax at source and transfer option *See Annex IX*

22. Current technology would enable an implementation of the tax at source and transfer model. In fact commercial providers already offer products which between them exhibit all the characteristics of the model. The major technological limitation at this point in time is around verifying consumers' jurisdiction as discussed above. The model is also flexible enough to benefit from future improvements in technology and the adoption of new technologies by business and consumers.

23. The main work required to implement this model is in attaining government agreement for the collection, transfer and remittance of consumption tax revenues. Technologies should also be considered that could mitigate possible increases in costs of tax administration.

---

8. Note that this analysis presumes a perfect world where no policy issues exist as to which jurisdiction's rules should be used for remittance and calculation or which classification is appropriate.

9. There is a recognition that a global tax system is impossible in the short term and improbable in the mid term, but global approaches to forms and methods coupled with government's assuming responsibilities for simplification to the extent possible and maintaining current, online accessible tables of tax could ease some of the compliance burden on business.

The trusted third party / clearinghouse option *See Annex X*

24. From a Technology TAG viewpoint, the TTP model is in large part identical to the tax at source and transfer model. The difference is that a trusted third party is charged with responsibility of collecting the tax rather than the local revenue authority.

25. The model raises the issues of achieving efficiency in implementation and examining how the costs / benefits of a consumption tax model could be shared between the parties involved in either the transaction or the collection of the resultant taxation revenue.

Combining the tax at source and transfer / trusted third party models *See Annex XI*

26. The strengths and weaknesses of these two models in some ways counteract each other. An alternate approach may be a hybrid one that takes parts of both the tax at source and transfer and the clearinghouse models. Such a hybrid approach is attractive from a technology perspective.

The Consumption Tax TAG's simplified interim approach

27. The Simplified Interim Approach (SIA) advocated by the Consumption Tax TAG provides a number of suggestions which would overcome many of the current issues associated with collecting consumption taxes on cross-border transactions. From the Technology TAG's perspective, SIA provides an integrated non-technological solution to the current consumption tax challenges. We have a great degree of empathy with the issues raised and advise that there is no technological impediment to this interim solution. We do, however, suggest that all possible efforts at simplification be undertaken and that a uniform user interface and forms set be developed to help facilitate implementation/use and to lower compliance burdens. Lastly, consideration of government maintained online tax tables, which are uniform in format, might also help facilitate the development of online look up systems for real-time tax calculation in cross-border transactions. More specific comments are set forth in the conclusions below.

Collection model conclusions

28. The Technology TAG sees the self-assessment model as impractical for business to consumer transactions.

29. The remaining proposals have strengths in particular elements but also have inherent weaknesses. For example, the registration model is strong in minimising government administration costs but business is left with a large burden in being able to correctly identify the consumer's jurisdiction to correctly levy a consumption tax. The costs involved in potentially registering and complying with up to 120 jurisdictions' tax systems are also abhorrent to businesses facing this prospect. The registration model is seen as a damper on the growth of e-business. This weakness from a business perspective is a strength of the tax and transfer model.

30. This leads to the concept of examining elements of the collection models to result in a stronger model. Such an analysis would involve determination of the technological alternatives for successfully implementing each of the six broad activities or modules shown in the model above.

31. To the extent that the Consumption Tax TAG and WP9 Sub-group have recommended to examine Registration Models as a near term solution, we would emphasise the following factors that may minimise compliance burdens:

- Develop standardised global procedures (*e.g.* forms, registration methods, etc.) and web access.
- Engage in simplification to the greatest extent possible.
- Explore ways to share compliance burdens, including by developing hybrid approaches.
- Understand the current limitations of technology to provide identification and verification.
- Work with business to explore technological improvements in identification and verification that have independent commercial utility to assure business investment and deployment; and
- Ensure that any interim registration options lead towards a more palatable collection model for the medium term.

Issues related to the work of the Professional Data Assessment TAG

32. Many issues which were considered for the PDA TAG revolved around the issues of verifying the location of the identity of parties to the transaction, where the parties were, when the transaction took place and the information inherent to or contained within the transaction. Since the PDA TAG looks at these transactions after the fact major issues were also raised as to the reliability of the records and systems which established the who, what, when and where of the transaction. While end-to-end virtual transactions were recognised to be the most problematic, concerns were raised about verifying electronic records of transactions. Since, under this section we will only discuss those issues which are significantly different than those raised in our evaluation of the collection models, the focus will be on when a transaction occurred and the reliability of records of the transaction. By way of analysis context, we point out that when reviewing the above factors, we also looked at issues of commercial reasonableness, costs of implementation and retention and comparison to non-virtual equivalents.

33. The PDA TAG highlighted two ways in which factors could be established. The first was to show that the record itself was worthy of credibility and contained sufficient information to establish the information in question. The second was to establish that systems, accounting methods and audit procedures were in place that were sufficient to provide evidence in the credibility of these systems. It was recognised that the latter case would be more applicable to larger businesses who hired or had on staff professional accounting experts who had reviewed systems and practices. In light of the greater concern with the smaller, unaudited practitioners, most of our attention was focused on those cases.

Establishing when a transaction occurs

34. The PDA TAG stated, in relation to consumption taxes, that it was necessary to establish the day when a transaction occurred. The two major technologies reviewed to establish transaction time were third party time stamping and document storage service providers and time stamp technologies (third party or system clock) included in e-commerce systems. While revenue auditors showed a preference for third party service providers that would both time stamp and archive documents, it was acknowledged that there was no reasonable commercial purpose for such service and the costs were prohibitive for the vast majority of online transactions.

35. Electronic commerce systems integrate order entries into databases. Databases provide relative[10] data entries keyed off the system clock. These systems can also be supplemented by references to external time stamping services. There were likewise, however, no commercial reasons for such services for the vast majority of Internet consumer transactions and there were concerns from revenue auditors that systems clocks and electronic records may be subject to alteration. In light of the presumed lack of programming sophistication by most SMEs it was considered that the greatest risk to alteration arose where third parties created programs designed to hide transactions or otherwise interfere with the proper functioning of the back end e-commerce systems.

36. Annex XIX discusses the technology aspects of electronic record integrity in more detail.

Need for training

37. There were concerns that there might be unreasonable expectations as to the ability of e-commerce systems to improve on the reliability of current paper-based and computerised accounting systems. These expectations resulted from the lack of training on e-commerce systems for auditors coupled with the lack of system models to compare. In a paper-based system, fraud is mostly discovered not by forensic analysis, but either by visible proof of changes or lack of congruity to established expectations derived from reviews of similarly situated businesses. In the case of electronic systems and transactions there is a need for auditors to understand the electronic traces which are left on systems as well as comparative models for Internet-based businesses.

38. Lastly, in tandem with work related to digital signatures, technologies for authentication and verification should be explored in relation to document reliability.

Proposed future work

39. Members of the Technology TAG have had some discussions around where the TAG's work should progress in the future. We believe that there are a number of factors which should underlie future work in this area:

- There is little tax revenue at stake currently in end to end online downloads.
- Technology, as existing and commercially diffused today, does not provide robust identification or verification methods for such downloads, however promising technologies were likely to be deployed in the middle term.
- There is a need to keep working on these issues as a priority in order to assure a level playing field for all market participants in cross-border transactions and the ability to collect revenue when such trade becomes more substantial.
- The emphasis needs to be on identifying solutions that could be deployed for effective compliance and we strongly caution against solutions that are incapable of compliance verification, overly burdensome in terms of cost or complexity or not supported by independent commercial rationales for collection of information.

10. "Relative" refers to the fact that data base entries are logged in relation to each other for the purposes of reconstruction of the database.

40. This background and our experiences to date led us to identifying the following areas as offering potential and warranting further examination:

- Examine viable short-term solutions which may not be technological solutions (*e.g.* the use of a merchant's internal databases).
- Further study of global IPv6 numbering including examination of the potential for geographic links to be inherent to IPv6 numbers.
- Complete a catalogue of third party tax services providers to document what is currently available and to provide information to merchants.
- Further study of digital signatures and what models may make sense for use by revenue authorities.
- Issues related to use and recognition of digital signatures in cross-border situations; roles of government and private sector in providing certification / registration authority services.
- More detailed review of the impact of wireless technologies and the impact of greater bandwidth availability.
- Ongoing monitoring to ensure that OECD directions correlate with changes in technology and commercial business models; and
- To identify new technology that could be harnessed to help address the taxation challenges of electronic commerce.

ANNEX I:
COMPOSITION OF THE TAG

The following people participated in the activities of the TAG and attended one or more of its meetings.

Full Name	**Company/Organisation**
Mr. Joseph ALHADEFF *(Business Co-Chair of the TAG)*	Oracle, United States
Mr. Stuart HAMILTON (until May 2000) *(Government Co-Chair of the TAG)* followed by Mr. Malcolm ALLEN *(Government Co-Chair of the TAG)*	Australian Taxation Office
Government representatives	
Mr. Blaise-Philippe CHAUMONT	Direction Générale des Impôts, France
Ms. Anne HUGUENIN	Direction Générale des Impôts, France
Ms. Isabelle OYARSABAL	Ministere des finances, France
Mr. Liam GALLAGHER	Inland Revenue, Ireland
Mr. Naoki OKA	Ministry of Finance, Japan
Mr. Kosuke YOKOO	National Tax Administration, Japan
Mr. Beat GISLER	Directorate of Taxes, Norway
Mr. Elvin HEDGPETH	Internal Revenue Service, United States
Mr. Terence LUTES	Internal Revenue Service, United States
Mr. Chun-Hsi LU	Ministry of Finance, Chinese Taipei
Mr. Mohd. Saian Bin HJ. RIDZUAN	Inland Revenue Board, Malaysia
Business representatives	
Mr. Oliver BLANK	EICTA, Belgium
Mr. Clive FARROW	Intel Corporation UK Ltd, EICTA
Mr. Robert COLE	Hewlett Packard, United Kingdom
Ms. Katrina DOERFLER	CISCO Systems, Inc., United States
Mr. Irwin ETTINGER	Citigroup Inc., United States
Mr. Lyndon WILLIAMS	Citigroup Inc., United States
Ms. Jeanne GOULET	IBM Corporation, United States
Mr. Sabri THAER	Mondex, United Kingdom
Mr. Jeremy HILTON	AddTrust AB, United Kingdom
Mr. Hirofumi HOTTA	NTT, Japan
Mr. Paul PUTLAND	British Telecom
Mr. Frank STEIMEL	Siemens AG, Germany
Mr. Peter WOOD	Ernst & Young, Canada
Mr. Takashi YAGI	Hitachi, Ltd., Japan

ANNEX II:
COLLECTION MODEL OPTIONS

1. The four options under consideration for the collection of taxes on cross border remote sales are as follows:

- Self-Assessment;
- Registration of Non-residents;
- Tax at Source and Transfer; and
- Withholding by Financial Institutions.

2. Each model gives rise to different combinations of the consumer / business (compliance points) and tax collectors (collection points) that are enrolled to collect the taxes involved. This is summarised in the following table.

	Tax Remitted to:	
Responsibility for tax collection rests with:	**(a) Tax office of the customer's country**	**(b)Tax office of the supplier's country (for subsequent transfer)**
(i) Customer	Self-assessment(Option No.1) or Trusted Third Party (Option No. 4) may provide assistance	n. a.
(ii) Foreign supplier	Registration (Option No.2) or Trusted Third Party (Option No. 4) may provide assistance	Tax and Transfer (Option No.3)
(iii) Tax and Transfer	Trusted Third Party (Option No. 4) may provide assistance	Tax and Transfer (Option No.3)
(iv) Trusted Third Party (any organisation):	TTP (Option No.4)	Tax and Transfer (Option No.3)
(a) Financial institutions used for settlement	TTP (Option No.4)	Tax and Transfer (Option No.3)
(b) Fulfilment & Delivery System Provider	TTP (Option No.4)	Tax and Transfer (Option No.3)
(c) Clearing house	TTP (Option No.4)	Tax and Transfer (Option No.3)

3. Technological solutions mean that the collection models under consideration are not necessarily mutually exclusive. A country might allow consumers to elect consumption tax collection points in certain cases. For example, consumption taxes may be collected by a supplier or by a trusted third party such as a clearinghouse. With respect to businesses, a large business may elect to register and pay the tax itself, as it may already possess a country structure with a permanent establishment. A small or medium-sized business may prefer to sign up with a trusted third party which could be a financial institution, a fulfilment and delivery system provider such as Federal Express, or a specialised clearinghouse. In addition, such a service provider might give rise to opportunities for achieving business and systems efficiencies by incorporating "tax compliance/collection" as a "unit module" in their global business structure. Such a

model would include various elements such as logistics, advertisement, bookkeeping, fulfilment, distribution and related functions.

4. Moreover, certain technological solutions may be viewed by government as a first step to the development of a longer-term solution. For example, the registration model, where tax is remitted to the customer's country, might be considered to be a precursor to a trusted third party model. Unfortunately from a business perspective, the business costs required of a local vendor to expand its operations in a foreign country, and meet the legal requirement as if it were a domestic entity, are substantial even if appropriate simplifications (based on possible technical solutions) are made.

5. For small and medium size businesses (SMEs), the investment in an international infrastructure needed to fulfil such a requirement would be prohibitive, and may in fact force vendors to operate locally and avoid taking advantage of the global opportunities presented by the "Internet". On the other hand, to exempt small and medium size business from tax obligations would create a competitive disadvantage for larger companies.

6. Therefore, in order to meet the needs of government and to encourage global business, a practical short term solution, proportional to the fiscal issue, is needed which would help policymakers implement a solution in steps. Such a stepped approach, however, could delay the implementation of tax collection objectives if the steps place the burden on business to continually meet changing government requirements which would lead to extensive re-engineering of business processes such as ordering, fulfilment and distribution systems.

7. Implementation of the ultimately agreed model to the sale of virtual products by businesses to consumers may form a viable short term starting point. This would allow development, implementation and evaluation of the preferred model, plus offer the potential for application to other electronic commerce facilitated sales in the longer term.

8. Important to any solution is the establishment of a "tax facilitator" and "tax simplification"[1]. A "tax facilitator" could take the form of a domestic government as in the tax and transfer model, or a "willing" third party, such as in the trusted third party model. With both a "tax facilitator" and "tax simplification", a local vendor or a even a consumer (in the self assessment model) would have the "ability" to comply with government regulations and engage in global commerce. In order to be neutral, efforts should be made to achieve a similar level of verification amongst implemented options.

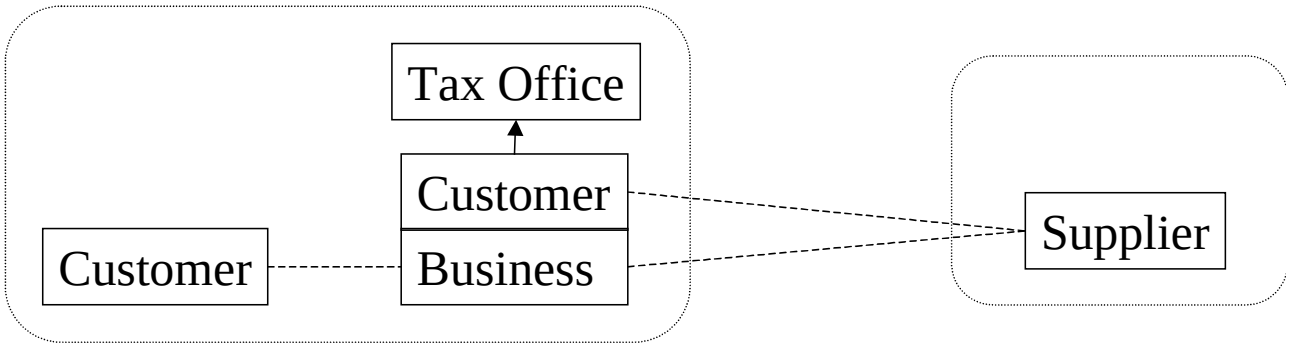
9. It would also be desirable for governments to clearly signal their intentions in relation to a long-term solution to allow businesses to work with government without the distraction of dealing with short-term proposals.

Self-assessment option

10. Under this model, tax is collected directly from customers (*i.e.* consumers) relying on a self-assessment process. Consumers would be required to determine the tax owing on imports of goods and services. This amount would then be remitted to their domestic revenue authority. While employed by many countries for supplies between businesses, few countries (Canada being one exception) have extended this model to include business-to-consumer transactions. In order to increase compliance and to

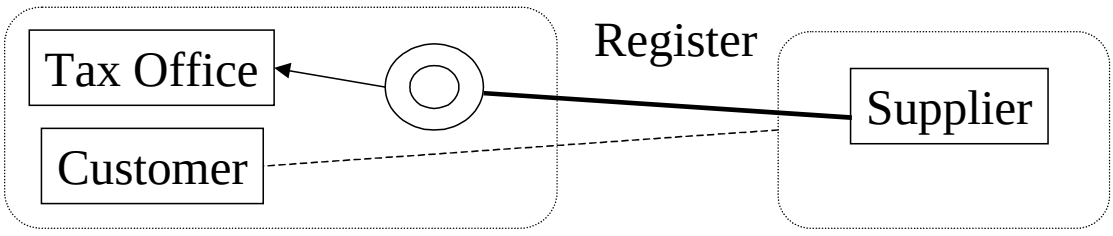
1. In the United States for example, the National Governors' Association have recognised the need for tax simplification and have initiated the Streamlined Sales Tax project (see www.nga.org/106Congress/SalesTax.asp and www.streamlinedsalestax.org).

make this option easy and transparent to a consumer, transaction software would be desirable, which would initiate a connection to a tax facilitator such as that provided by a trusted third party. Such a trusted third party would do the tax calculation, invoicing, collection and remittance to the government. On the other hand, a more simple approach would be to require payments due for consumption tax to be included in an income tax return (certain states in the United States are utilising this low-tech alternative).



Registration of non-residents option

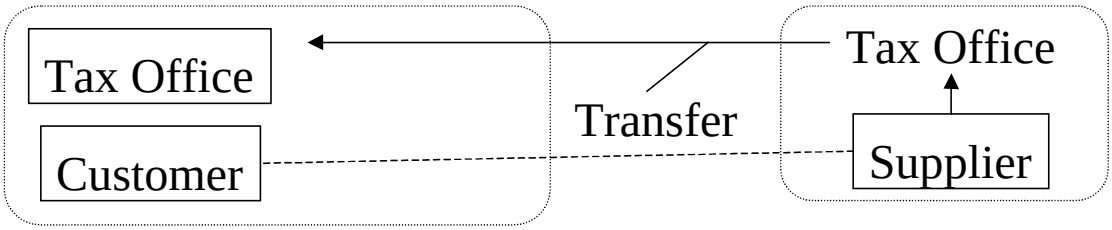
11. Under a registration option a non-resident supplier is required to register with the revenue authority in the consumer's jurisdiction and collect and remit consumption taxes to that revenue authority. Businesses would be required to register in every jurisdiction in which they sell and deliver products. Foreign businesses would then be treated the same as domestic businesses for consumption tax purposes by the revenue authority in each jurisdiction in which they trade. An example of this is the registration mechanism applied on telecommunications services in the European Union. Due to the difficulty for SMEs to comply with over 100 VAT regimes, the tax calculation features of the tax and transfer model and the trusted third party model may assist a vendor to comply globally were such a requirement to exist legally. Unfortunately, the ability of a tax jurisdiction to enforce such a tax regime beyond their borders will be spotty at best, leading to market distortions and inequalities.



Tax at source and transfer option

12. Under the tax at source and transfer option, a business would collect indirect taxes on exports to non-residents at the rate payable in the consumer's jurisdiction. This amount would then be remitted to the business' domestic revenue authority, for on-forwarding to its counterpart in the country of consumption. Business only has to deal with their local revenue authority. SMEs in the tax and transfer option could also rely on a trusted third party model to facilitate compliance with tax rules from the over 100 VAT regimes.

13. This particular option is used for example, to collect domestically the United States Highway Use Tax on Trucks and in Switzerland for the collection of withholding taxes on interest payments.



Trusted third party (TTP)

14. A trusted third party (TTP) is a generic term, which could refer to any organisation that is performing a task for merchants, consumers or governments. A TTP could take the form of a financial institution, a fulfilment and distribution system provider, or an independent clearinghouse. TTPs should not be mandated on any intermediary or class of intermediaries. Instead, companies should volunteer to become TTPs based on market driven commercial viability to meet legal and other concerns while providing appropriate incentives for all of the parties involved.

15. Under the TTP option, a TTP (other than a supplier) would have to rely on the supplier to classify its catalogue according to a standard classification system, which would have to be put in place. The supplier would have to rely on the jurisdictional information it obtains from the customer until suitable verification mechanisms are agreed. The standard classification system would require computerisation and suitable databases, which could be accessed by relevant parties. Such databases would be used to eliminate the need for duplication and redundancies, which would otherwise result when suppliers and TTPs require similar information, the former to close the sale and the latter to collect the tax. Such duplication would impose an additional burden on the e-commerce economy that would not be present in the traditional physical goods economy.

16. The supplier would remain liable for the accuracy of his classifications. In order to reduce errors in the system and therefore minimise its liability, the TTP would rely on governments to verify its tax collection module in order to certify that the tax rates, tables, reporting etc. meet each government's legal requirements.[2] In addition, the TTP would be required to meet all privacy obligations that it has undertaken and any legal requirements that it is subject to within its jurisdiction. In fact, in order to perform its task, a TTP would require only the tax jurisdiction of the consumer and a classification of the item purchased. The TTP would not need personal information of the buyer nor would he need to access the customer's personal files to determine tax jurisdiction, provided that a reliable mechanism could be agreed upon to provide such information.

2. Authentication technologies could be used to lessen the possibility of spoofing or otherwise fraudulently representing the site.

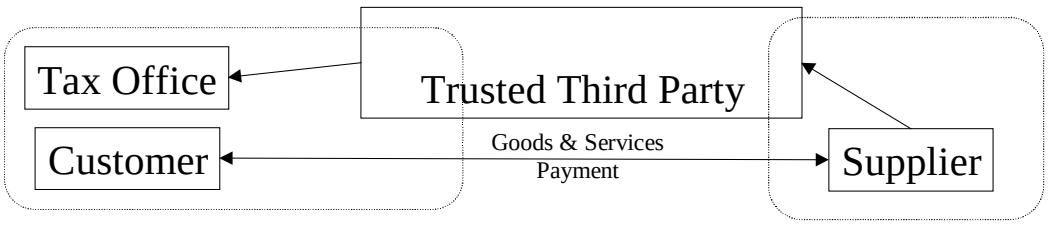
17. As a subset of the TTP, the Consumption Tax TAG and the WP 9 Sub-group have suggested that a financial institution or a credit card company could be enlisted to collect the consumption taxes for which liability arises from electronic purchases. One of the reasons for this suggestion is that financial institutions already facilitate the financial transaction between the business and the consumer. It was also suggested that the financial intermediaries would then remit these amounts to the revenue authority of the country of consumption.

18. A number of financial institutions or credit card companies have already indicated that they do not collect the necessary data to perform the tax collection task. In fact, financial institutions claim that they are not engaged in the business of selling goods and taxable services and therefore are not equipped to collect and remit consumption taxes. Financial institutions believe that the responsibility for obtaining information to determine jurisdiction of the consumer and the collection and remittance of taxes rests with suppliers who are directly involved at the point of purchase. As a necessary part of any on-line purchase of physically delivered goods and services, the customer furnishes relevant information such as name, address, telephone number, e-mail address, description of product, catalogue, product number, quantity, price, and method of payment to the supplier. In addition, the supplier generally has a more flexible structure where any payment method can be used. Many of these indicia may likewise be available to the supplier in virtual transactions. For these reasons, according to financial institutions, suppliers are uniquely positioned to use information to determine jurisdiction and taxability.

19. With respect to financial institutions, most of the essential information for determining jurisdiction and collection of tax are not available at the point of purchase. The credit card payment authorisation process does not involve access to customer's address, telephone number, e-mail address, and description of product and catalogue product number. Change in the authorisation process would require fundamental systems modifications affecting issuing banks, merchant banks, credit card associations, credit card holders and other parties.[3] Financial institutions, as well as domestic suppliers, would have to make significant changes to their corporate infrastructure in order to act as a TTP. The challenge is to create a "value proposition" that would make such a significant financial commitment, a viable proposition to the governments or businesses who ultimately incur this expenditure.

20. In addition, any sharing of customer's information with suppliers raises significant issues in relation to security, fraud and privacy. This is a major area of concern and sensitivity for payment facilitators. . For a more detailed review of credit card business models, customer issues and rationale for the conclusions that credit card companies are not "*the"* appropriate TTPs, please see Annex IV.

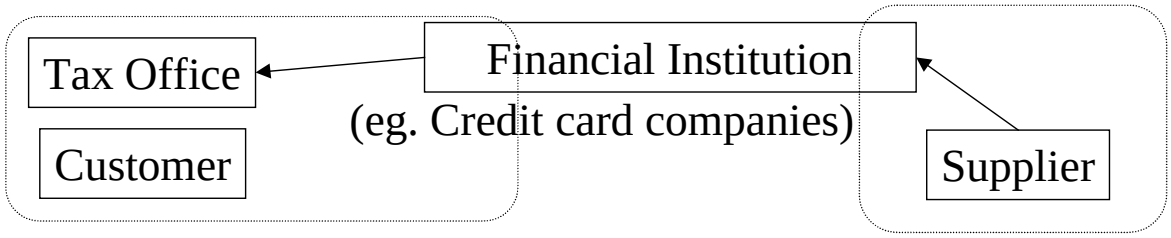
21. Therefore, under the TTP option, team work among suppliers, financial institutions, as well as government would be required. The logical structure of this option has many similarities with a tax at source and transfer model. The differences lie in who assumes responsibilities for various functions.



3. See Annex IV for a more detailed analysis of the credit card industry.

Withholding by financial institutions

22. The Technology TAG sees this model as being one variation of the TTP model discussed above.

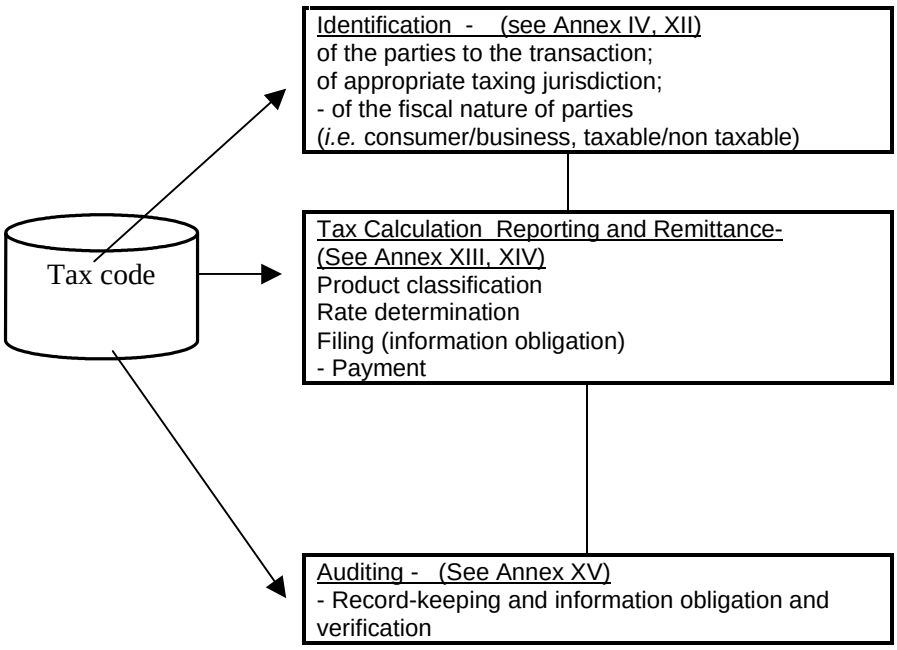


Common elements and their linkage to business practice/technologies

23. For each of the options the following common elements exist in the levying and collecting of indirect taxes on various transactions:

- Identification of the parties to the transaction and appropriate taxing jurisdiction;
- Tax calculation - product classification and rate determination;
- Reporting and remitting of taxes to appropriate agency; and
- Compliance verification.

This is represented in the following diagram:



Business need for identification

24. Internet vendors have a business need to manage their exposure to fraud risk and the credit risk of potential customers. One way of dealing with this is to request identification details from the potential consumer. The information supplied may then be cross-checked with other indicia, which would be made available to the vendor. This is rarely done today. Competitive business models on the Internet are built upon the premise that similarly priced competition is only "one click" away and that consumers do not wish to provide needless information or be presented with more screens than necessary. Consumers are thus afforded the least intrusive method of ordering and registration with information collection screens kept to a minimum. Privacy concerns are also pushing businesses to limit information collection and begin storing as much information in anonymous form as possible. Governments must address the underlying tension between the needs of tax authorities to identify consumers and the requirements of consumer protection and privacy authorities to allow consumer to opt out of personal information collection.

25. Banks however, for fraud control purposes, perform a check between the credit card number and the billing address, but do not necessarily share this information with the vendor who could then check the shipping address provided by the customer. There are also issues of real time application, the vendor card check merely goes to the back end clearing system for validation of credit available, it is not routed back to the issuing bank. For a fuller treatment of the technological issues related to credit clearing, please refer to Annex IV. Although business would like to obtain as much information as possible from their customers, mere self declaration of the consumer would probably be adequate for business needs and the higher degree of accuracy or verification desired by government for taxation would probably not be required to accomplish, and may actually impede, the business needs of the transaction.

26. The European e-business Tax Group (EeTG) position paper on invoice requirements specifies "identity of the customer" as one of their common invoice elements. In the case of a consumer, this would consist of the consumer's name and address. While there is no surety that a consumer in an electronic transaction of an intangible product would provide an accurate address, this is an indication of businesses' need for this information. There is clearly a business need for an address in cases of online shopping for physical goods. That need, however, minimised, if not vitiated where the goods may be downloaded directly over the net by the consumer. In the case of a subscription type of service, an e-mail would also be required. While businesses may desire to more about their consumers, the issues of privacy and permission marketing have begun to temper companies inquiries relating to personally identifiable information. Consumer wishes may conflict with business needs and some have expressed a concern that the concept of neutrality should exist with respect to disclosure of information. As it is possible today to purchase from a traditional store without divulging information on identity, the same should hold true for Internet commerce. Thus any efforts at identification will be controversial in some countries and in the Internet community.

27. The solution for taxation purposes may lie in using other indicia to verify the consumer's self-declaration of their jurisdiction rather than attempt to establish or determine jurisdiction.

Technologies/methods

28. A major issue in applying consumption taxes in an electronic commerce environment is the determination of the consumer's jurisdiction. This is particularly an issue for the trade of intangibles, which may be supplied through an electronic download. This mechanism often means that the business currently requires little more than the consumer's credit card details to facilitate the trade. The issue faced by revenue authorities is to collect sufficient information to identify the consumer's jurisdiction while minimising compliance costs for both the business and the consumer.

29. Technology itself is the logical method of meeting the needs of all those involved in these transactions. A number of technologies/methods present themselves as potential aids to identifying the consumer's jurisdiction.[4] The main contenders are digital certificates, credit card number, credit card billing address, IP address, and self-declaration.[5]

30. All of these identifiers have some, if not significant, limitations.[6] There is also a time element involved as technologies evolve and are taken up by businesses and consumers. If digital certificates become commonplace as expected by their proponents and governments take the necessary steps to ensure their validity for taxation purposes, there is little doubt that this will provide the best longer-term solution.

31. However a combination of existing technologies and approaches should result in a high level of accuracy of jurisdictional identification in many cases. Reliance on one technology would result in a lower level of accuracy and the practical solution is for a combination of these techniques to verify/check identification to be implemented by parties to the transaction. A high standard of identification, over and above customer declarations would increase the costs of the transactions and needs to be evaluated for its economic impact in relation to the benefit derived by governments. In most situations the required level of jurisdictional identification for taxation purposes is limited to the country level and the solutions proposed in this paper have sufficient robustness while minimising the compliance costs of businesses and consumers.

Compliance verification

32. As with any collection model, it will be important for adequate controls and audit trails to be built into the implemented version. Annex XV provides an analysis of the audit trail options available.

4. See Annex IV for a "Technology Primer for Identity of Parties and Classification".

5. See Annex IV for a discussion of these technologies and their limitations.

6. See Annex IV for an comparative evaluation of the jurisdictional identification technologies.

Summary analysis of collection models

Tax Collection Option	Effectiveness	Effect on consumers	Compliance Burden vendor	Administrative Burden	Feasibility
Self assessment	Difficult	Large burden	None	Large burden	Not acceptable to revenue authorities
Registration of non-residents	Difficult	None	Large burden	Large burden	Not practical on a global scale
Tax at source and Transfer	Good as only have to deal with revenue authority in business' home jurisdiction.	Neutral	Small additional burden. One set of books.	Small additional costs. No primary concerns.	Yes, requires agreement amongst states and local governments. Throwback rule may discourage exports.
Clearinghouse/ trusted third party	Good as tax model is included in an end to end vendor system which is needed for cross-border business	Neutral	Start up costs exists, but future benefits due to efficiencies, consolidation, automation and minimisation of errors may yield substantial benefits which will offset the costs.	Start up costs exists, but future benefits due to efficiencies, consolidation, automation and minimisation of errors may yield substantial benefits which will offset the costs.	Yes certain vendors are searching today for integrated end to end facilities. Global teamwork required!
Hybrid tax at source & transfer / trusted third party	Good as above	Neutral	Small additional burden. One set of books.	Some additional costs.	Yes – see above

Collection models' roles and responsibilities

	Collection Model				
Module	**Self-Assessment**	**Registration of Non-residents**	**Tax at Source & Transfer**	**Trusted Third Party**	**Hybrid**
Registration	Customer with Approved Registration & Certification Authority	Business with Govt approved Registration & Certification Authority	Business with Govt approved registration process	Business with Govt approved registration process	Business with Govt approved registration process
Purchase request and classification of catalogue	Business	Business	Business	Business	Business
Customer Identification	Based on approved information supplied by customer	Customer jurisdiction verified in purchase transaction	Customer jurisdiction verified in purchase transaction	Customer jurisdiction verified in purchase transaction	Customer jurisdiction verified in purchase transaction
Tax Calculation	Data from business and global tax database (revenue authority required to maintain)	Data from business and global tax database (revenue authority required to maintain)	Data from business and global tax database (revenue authority required to maintain)	Data from business and global tax database (revenue authority required to maintain)	Data from business and global tax database (revenue authority required to maintain)
Collection / Remittance	Customer remits to customer's jurisdiction	Collected by business for remittance to customer's jurisdiction	Collected by business' revenue authority for remittance to customer's jurisdiction	Collected by trusted third party for remittance to customer's jurisdiction	Collected by business' revenue authority for remittance to customer's jurisdiction
Compliance Verification	Customer's revenue authority	Customer's revenue authority	Business' revenue authority	Business' revenue authority	Business' revenue authority

ANNEX III:
JURISDICTIONAL VERIFICATION

Introduction

1. One of the issues which seems to have created much debate arising from the Technology TAG's "Technological Perspectives on Consumption Tax Collection Models for Cross Border Electronic Commerce Trade" is around the details of a jurisdictional verification model.

2. The part of the collection model focused on by this paper is the "Customer Identification Module". The specific area which needs expanding upon is the function described as "Get customer's IP# & credit card number". The associated issue is what to do with these details when they are received.

3. In order to advance these discussions, we propose a model for how a business model could operate to collect the requisite customer information to verify the customer's jurisdiction. It must be kept in mind that the scenario in which these details would be used is only:

- B2C transactions;
- Involving cross border purchases of electronic goods; and
- Where an acceptable digital certificate verifying their jurisdiction is not offered by the customer.

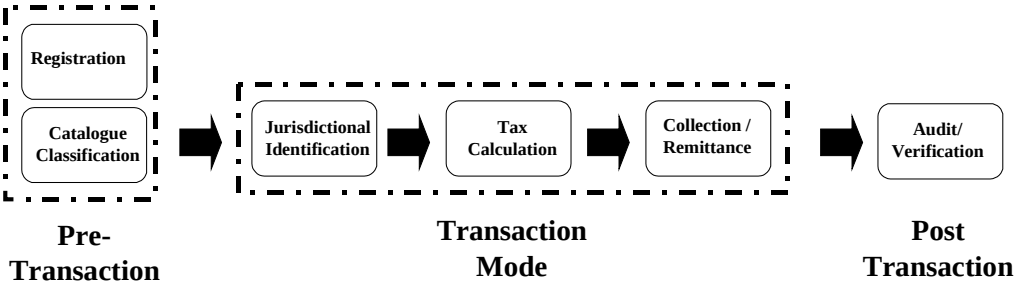
EU model

4. Before discussing these issues, a short note in relation to the proposed EU model. While that model outlines how and when tax needs to be paid on electronic supplies into the EU, it does not establish how the foreign business satisfies either their local revenue authority that the product was an export or the EU revenue authority that it was a supply into the EU. It merely states that "a decision will be required on the jurisdiction"[1] and discusses some of the issues, noting the value in using credit card numbers for jurisdictional verification.

5. In this regard, attention is drawn to the six modules of a successful implementation of a collection model as detailed in the primary paper. See figure on next page.

6. The solutions discussed in this paper are therefore equally applicable to the EU's suggested model or any of the other models that have been considered in the OECD discussions. The point is that a successful implementation requires a solution to all six of the identified broad activities or modules.

1. See page 8 of the Commission of the European Communities' Proposal for a Council Directive … as regards the value added tax arrangements applicable to certain services supplied by electronic means available at: europa.eu.int/comm/taxation_customs/proposals/taxation/com349_2000/com2000_349en.pdf.



Safe harbour

7. The purpose of employing these technological solutions is to provide business with a safe harbour for zero rating the export of electronic goods for consumption tax purposes. [2] We need to get to a solution which provides business with guidelines as to what a revenue authority would consider to be sufficient evidence for them to zero rate an electronic supply.

8. The issue of digital certificates is seen as a mid term solution. Suffice to say that if digital certificates become a pervasive part of B2C electronic transactions they may provide the jurisdictional evidence that tax authorities are looking for[3]. Underlying the integrity of a digital certificate however is the evidence required by a Registration Authority in verifying the claimed identity of the application. Not only is this something that revenue authorities would need to specify as to the level of evidence required, jurisdiction is currently not a standard field on the majority of digital certificates.

IP numbers and self declaration

9. We had initially been working on the premise that both of these solutions offer us at least 60-70% level of reliability as at the consumer's jurisdiction. The issues involved in these technologies are outlined in Annex IV.

10. It would seem that in the (idyllic!) cases where we were able to identify two or more technologies to offer us a high level of reliability, a vendor should be able to depend upon the consumer providing evidence of one to be provided with a safe harbour. In this regard it needs to be recalled that we would be

---

2. In light of the small amount of overall commerce that is end-to-end electronic, the desire of EU Tax authorities and businesses to create a level playing field for such transaction across different VAT and non VAT jurisdictions and to address the problems of identifying and verifying jurisdiction, some Businesses have suggested that all end-to-end e-commerce should be zero rated for a fixed period of time after which there should be a gradual ramp up to market rate. It is argued that this would provide an immediate leveling of any competitive price disadvantage related to VAT, would provide time to develop a workable solution from both a policy and technology perspective and, due to the fractional percentage of commerce which this represents, would not significantly decrease taxable revenues.

3. There is little evidence at this point to indicate that consumers are likely to move towards digital certificates for online purchases or that vendors will develop a business need for certificates to be tendered as part of an online purchase. SSL currently provides sufficient security for both parties. It seems more probable that the use of digital certificates will become more pervasive as part of systems used by consumers where they will generally be unaware of the fact that a certificate is being used as part of the operation they are engaging in. An example is the ATO's Internet lodgment of taxation returns where the taxpayer downloads ATO software that incorporates a single use digital certificate that the taxpayer would not even be aware of.

initially asking the consumer to self declare their jurisdiction with the IP number or alternate mechanism examined to verify that self declaration.

11. So the vendor could choose to use a traceroute on IP numbers or could use information provided from marketing communications or other consumer jurisdictional sources to verify the self declaration. They would then be expected to maintain a record of this information and the jurisdiction indicated to meet their taxation obligations. Of course, the lookup would also need to match the consumer's self declaration of their jurisdiction.

Exceptions

12. It does not seem appropriate to always accept IP numbers as evidence of jurisdiction. We are aware of a number of scenarios where these technologies have limitations. It is proposed that where the result of a trace or lookup is within a limitation zone, then this should not be acceptable evidence for the business to rely upon in order to take advantage of the safe harbour offered.

13. For example, if the business generally relied upon IP traces but the consumer was using an anonymiser service which effectively hid their identity, they could not rely upon the IP trace for that transaction. They would then need to look at alternative verification methodologies to verify the consumer's jurisdiction if they are to zero rate the export within the terms of the safe harbour offered.

14. It is proposed that the exceptions from reliance on each of these two technologies should be as follows:

IP Number Trace Result	Rationale
Anonymiser used	The consumer may have a number of valid reasons for protecting their privacy however it means that an IP number trace is unreliable and the vendor should use an alternative instead.
IP number is in a listed "haven" country	May be a genuine case but also possibility that consumer is using an anonymiser or proxy server to portray themselves as being in the listed country. Again the IP number trace loses reliability and an alternative should be used.
IP number belongs to AOL or a similar aggregator of Internet access across country borders	AOL and similar providers provide an IP number trace result which reflects AOL's single access point to the Internet rather than the consumer's location. This may be a case where direct negotiation with AOL may help identify a solution. Alternatively the vendor will have to rely on an alternative methodology.
IP number belongs to a corporate known to aggregate Internet access across country borders	Similar situation and solution as the AOL case. However for large corporates, the IIN lookup may also prove unreliable due to a single source of credit cards for the international operations of the corporate group. (In fact the larger corporates often have their own IIN range allocated.) Will also be issue of whether transaction is actually B2B rather than B2C which may not be apparent from vendor's position. More difficult to successfully resolve but question as to quantity of trade that this may represent and whether it is therefore worth worrying about.

When no verification is possible

15. There will be some situations where the IP number trace or other corroborative information will be insufficient to verify the consumer's self declaration of jurisdiction. This may be because the consumer

is not being truthful in their self declaration. Alternatively it may be a combination of the factors listed above where the technologies have limitations.

16. Whatever the reason, this would be a situation where the business could not be offered a safe harbour to zero rate the digital download of the electronic products. The basic fallback position would then be that as the business has no proof that the supply is an export, the supply would attract the consumption tax rules / rates of the business' own jurisdiction. That is, the supply would be taxed as a domestic supply.

17. If the business is not happy with that result, they may have other options available to them, depending upon how this fits with their business model. These would include:

– Bearing the domestic consumption tax themselves; or

– Undertaking other verification checks to establish the jurisdiction of the consumer. (If other checks are shown to be reliable then they could be added to those accepted for the safe harbour offered by the revenue authority).

ANNEX IV:
TECHNOLOGY PRIMER FOR IDENTITY OF PARTIES AND CLASSIFICATION

1. Four different models of applying consumption taxes to digital goods have been described by the Working Party 9 Sub-group on Electronic Commerce in their Working Paper on Tax Collection Mechanisms. These models are directed at ensuring that digital goods purchased over the Internet attract consumption taxes in the same manner as when purchased in a traditional transaction within the consumer's jurisdiction.

2. All of the models have in common the need for the vendor to have some knowledge of the purchaser to achieve this equivalent tax effect. This Annex introduces the concepts of

- Identification and authentication;
- Current and future supporting technology that may be used to facilitate the models; and
- Technology that might be used in assisting in the classification of digital goods to determine applicable tax rates.

Identification and authentication

3. **Identification:** Common to these models and Internet commerce in general is the need to know the identity of the parties to the transaction..

4. **Authentication:** When someone declares an identity there is usually a need to establish that the party is who he, she, represents himself, herself, to be (called, for the purposes of this paper, authentication). Authentication can be done with various degrees of confidence depending on the business need. Once the identity is known and confirmed, other associated attributes may be required, such as physical location, country of residence, and whether registered with the country's tax authorities.

5. The table on the next page sets out a framework outlining various identification and authentication techniques. Most systems consist of at least one of the four identification techniques.

What techniques are available today?

6. Over the next decade, digital certificates of some kind may become common. In the meantime, what techniques could be used today to identify the tax jurisdiction of consumers?

7. **Self-declaration as Basis of Jurisdiction:** An individual might simply say that he or she is not resident in the jurisdiction of the vendor when buying digital goods. Because digital goods are delivered over the Internet without the need for an accurate physical address to match the goods with the purchaser, it would be easy for users to declare that they are outside of the vendor jurisdiction. A number of commercial Internet sites do not require the purchaser to disclose a physical address.

Technique	Examples	Comments
1. Password-based systems: *something you know*	Password, mother's maiden name, PIN number, information on line x of tax return, billing address on credit card, birth date	According to Forrester Research, Inc., typical employees today must remember 15 or more passwords. This issue could be alleviated with the use of digital certificates or smartcards.
2. Physical tokens: *something you possess*	Physical tokens such as a building access card, bank card, credit card, smart card with embedded chip (e.g., Mondex), RSA's secure ID (which has a constantly changing unique token)	Often used in conjunction with "something you know," such as a password. Smart cards and certificates are still immature technology
3. Biometrics: *something you are*	A person's unique physical traits, such as fingerprint, voice, eyes, hands, or face	Not widely deployed today but expected to become increasingly common over the next decade in high-security environments, but unlikely to become widely used given cost and privacy concerns
4. Location: *where you are*	Systems using the Global Positioning System (GPS) or GPS-like techniques to authenticate users based on where they are	

8. **Credit Card Address / Number as Proxy of Jurisdiction:** For consumer transactions over the Internet, credit cards are likely to remain the dominant form of payment in the majority of countries[1]. While the concept of matching a credit card number to the country of residence was originally thought to have promise, further investigation demonstrated that there was no numerical BIN correlation to geography, no uniformity across credit card clearing systems, and significant privacy and business model reasons why the information could not be shared. For further information, refer to Annex IV. **IP Address of Purchaser as Proxy of Jurisdiction:** The IP address of the individual as communicated to the vendor by the user's browser could be checked to see what country it likely came from and whether this is consistent with other correlative information provided by the customer. When a consumer is using the Internet, they will have an IP address, often dynamically allocated by their ISP. The Internet *traceroute* command could be used by the business to determine the physical location of the consumer. In some, if not a majority of situations, the traceroute result could be sufficiently precise to enable the consumer's taxation jurisdiction to be determined.[2]

9. The use of traceroute to identify the location of the consumer is already used by businesses who are prohibited from trading certain items cross borders (e.g. online casinos and sellers of software incorporating advanced cryptography features, anti-hacker bodies and law enforcement agencies).[3] These

1. In some countries, such as Japan, credit cards are not the predominant payment systems for cultural reasons.

2. *Traceroute* enquiries are readily available through many sites on the Internet. Annex XVI presents a visual *traceroute* enquiry on the United States Advisory Commission on Electronic Commerce homepage using Visual Route which also presents a visual map of the route between our ISP in Canberra and the ACEC in Richmond, VA. This program is available for purchase from www.visualroute.com.

3. A recent example is that of Emusic who appear to have incorporated traceroute functionality into a tracking system built to counter Napster users infringing on music copyrights King, Brad; Emusic Tracks Napster Naughties; available at http://www.wired.com/news/print/0,1294,40316,00.html.

tracing technologies are used in conjunction with a cross check of identification against a denied parties list. While the systems appear straightforward on the surface their design and installation can be both costly and disruptive to the business. The time and computing power involved in executing a traceroute query is minimal in the context of the overall transaction time, but there is the question of the overall overhead added to aggregate electronic commerce transactions[4]. This is however an issue for any online method of jurisdictional verification. A more critical issue is the significant number of transactions which may yield indefinite results should these have to be reviewed in a manual process, eliminating the benefits of real time processing. The challenge will be to agree on the business rules for automatically dealing with these indefinite results. Any potential delays or greater system costs may also result in a competitive disadvantage should other vendors in other countries not require these procedures. On the Internet, competition is only a click away and geography is becoming more irrelevant.

10. While new IP tracing/tracking technologies (TraceWare by Digital Island) seem to offer greater promise in this regard their utility is limited by certain trends in Internet architecture. Digital Island does not disclose the technology behind TraceWare, but claims it to be more effective and time efficient than either DNS information generally or TCP/IP traceroutes (traces route "hops" to origin). A cursory reading of Digital Island's promotional material indicates a 96% accuracy rate as to geographic origin. The FAQ, however, places that number in question. TraceWare does not seem to effectively penetrate the AOL network, may have trouble with corporate proxy servers and may not properly account for "access oriented" ISPs (that funnel through a bastion/proxy server). All of which represent growing trends in centralisation of access and security. It is equally unclear what the new introduction of gTLDs will do to these evolving tracing technologies.

11. While IP addresses may be accurate most of the time, they may become increasingly problematic. For example, the Consumer's Association recently recommended that consumers use an "anonymiser" service to disguise their IP address to the vendor so as to protect their privacy. Thus an "anonymiser" located in a tax haven country would show the consumer's residence to be the tax haven country if the IP address alone were used.

12. While these concerns are valid, most consumers currently do not avail themselves of anonymiser services and there is no evidence to indicate that their uptake of these services is likely to increase. Many anonymiser services will show identifiable IP numbers that can be allowed for by a throwback rule applying the tax rules of the business' jurisdiction to the purchase of virtual goods in these events[5]. ZeroKnowledge's anonymiser system is less easily dealt with but again the rate of uptake is not known to be significant. Wired.com reports that "very few people appear to have paid the $49.95 a year to cloak their

---

4. For example, an IP address trace is much quicker than that involved in verifying the authenticity of a digital certificate with the certificate's issuer or in gaining transaction approval from a credit card supplier. All that a traceroute enquiry is doing is sending a series of packets between the merchant's and the consumer's servers. It should also be noted that the technology, including source code if required, is freely and commonly available. It is a standard UNIX command and is already incorporated in all operating systems as well as enhanced versions available online and for commercial purchase. Online versions including www.samspade.org and commercial products such as VisualRoute (www.visualroute.com) include traceroute as part of a suite of online tools which may include enhancements such as map depictions of the traceroute results.

5. A throwback rule has been criticised by some who claim that it provides an incentive for businesses to claim that they can not determine the location of consumers who come from higher tax jurisdictions. This would enable them to supply the product at the lower rate of the business' local jurisdiction. It is suggested that this risk is very small. The potential savings for consumers are fairly small compared to the risk of the business being subject to penalties in their local jurisdiction. An algorithm check could be used by local tax authorities to provide a simple compliance test to ensure this practice does not become prevalent.

online activities from prying eyes."[6] It is unlikely that attempts to avoid consumption taxes would attract significant numbers of consumers to anonymisers.

13. Consumers who use AOL or similar providers are assigned IP addresses without regard to their country location. This problem may be particularly prevalent in North America where both Canadian and *US* consumers will share the standard AOL IP address but have different taxation liabilities. While inquiry with AOL on this matter is possible, there are legitimate business reasons for their choice of architecture which have no relation to tax administration. The Technology TAG believes that the most workable solutions to these issues are ones where there technologies that are useful for tax administration have commercial purposes and reasonableness. Another issue for AOL would be its desire to respect the privacy of consumers. More and more businesses are providing some aspect of anonymity to consumers and giving consumers a greater voice in orchestrating the relationship with the company. Many of these efforts are collectively referred to under the rubric of "permission based marketing".

14. Consumers using computers at work to acquire goods may also not have reliable IP addresses. For example, some multi national corporations use a single Internet access point for their worldwide operations. Thus the IP address of that firewall or proxy server is at the access point will be communicated, which will not necessarily correspond with the country location of the consumer. Any significant taxation risks arising from this practice may require individual negotiations similar to those proposed above for AOL. It should be noted that corporate aggregation of Internet access is a growing practice to enhance security. No data on the level of Internet purchases through employer provided Internet access have been identified.

15. The limitations of IP address traces such as the use of anonymisers and corporate aggregators are inherent to the technology. It is unlikely that these limitations from a jurisdictional verification viewpoint will be solved using technology. Instead there is a need to look for non-technological solutions. Another inherent problem in IP lookup technologies is the impending change in the IP standard from IPv4 to IPv6. Vendors are reluctant to invest in any system that has an assured short term obsolescence and are unwilling to invest in technologies using the new standard until they are in wider deployment. This may raise the question of governments funding the development of the required technology.

16. The current system of IP addresses, IP4, is expected to be replaced in the next decade by IPv6, which will have the capability to use the Media Access Control (MAC) address, which is permanently assigned to a network card, to generate a unique IP address. Once IPv6 becomes popular, users could potentially have unique IDs. Even though each network card vendor is provided with a set of MAC addresses to burn on their network cards, there is nothing binding in the MAC address. A particular MAC address cannot be inextricably linked to a given computer or other device as the Network Interface Card (NIC) can be moved.

17. The IPv6 addressing structure and allocation scheme as currently proposed is strictly hierarchical, but not geographically hierarchical. It has been specifically designed to be more logically hierarchical, and on a network basis not a country/geographical basis.

18. Thus it seems that IPv6 numbers could be used to determine top level network provider used, but would not be able to determine geographic location. This is essentially the same basis as IPv4 - which means that there would be a pseudo geographical link as ISP's tend to be country/region specific (at present - this will probably breakdown over time with increased telecommunications deregulation).

---

6. Declan McCullagh, "Privacy Firm Tries New Gambit", 1 November 2000, available at http://www.wired.com/news/print/0,1294,39895,00.html

19. The real question is if allocation were done on a geographic/regional basis (*e.g.* Europe, US/Canada, Oceania etc) what would be the overall disadvantages and advantages - policy aspects need to be brought into the frame of reference.

20. Our research on this issue has not proved that successful in obtaining contacts or more information on the planned IPv6 rollout. We have also struggled in getting responses from those working on other issues, such as those countering denial of service attacks, who may share our interests in geographical allocation of numbers. It is also possible that those working on those issues outlined in the issue, such as those involved with intellectual property, have not considered such a solution. A proposal for a combined approach from those who may have similar needs may be worth exploring.

21. It appears that the Internet Engineering Task Force (IETF) is the body controlling the work on IPv6 that we need to work with. We therefore recommend that a formal letter from the OECD to the IETF is the appropriate course of action to progress this issue.

22. For more information regarding IPV6 please refer to:

- http://www.ipv6.org
- http://www.ipv6forum.com
- http://www.ietf.org/html.charters/ipngwg-charter.html

23. From the revenue authorities' perspective, it would be ideal if the assignment of new IP addresses be made more strictly on a country basis and enforced. From businesses' perspective, a more rigid country allocation system might help enforce regional pricing policies. Currently there are three regional registries for the issuance of IP addresses:

- AP-NIC – for the Asia-Pacific region
- ARIN – for the Americas, Caribbean, and Africa
- RIPE-NCC – for Europe

24. For more information on the allocation of IP addresses please visit the Assigned Numbers Authority web site at http://www.iana.org

25. Another approach would be to embed a unique serial number in each computer processor. Intel tried this with the introduction of the Pentium III chip. However, significant negative press on the privacy issues raised by this approach forced Intel to drop this policy. The privacy issue was partly fuelled by the potential for using this unique serial number to track these processors through a central database.

26. **Wireless Technologies**: Internet access via wireless mobile devices such as mobile cellular phones and handheld computing devices is a growing medium. While not expected to be a major electronic commerce facilitator in the next two years, wireless access should be considered in any systems being planned. Within that time frame the penetration of wireless devices should exceed that of PCs. Internet access devices will have limited form factors and screens not suited to large information disclosures and exchanges. Any tax administration functionality will have to be tailored to operate in this environment.

27. The Wireless Application Protocol (WAP) is becoming the current industry standard for wireless Internet access, though other more advanced "third generation" protocols are also being developed. The

wireless device will commonly communicate with a WAP proxy server, which translates WAP requests to WWW requests, allowing requests to be submitted to a Web server.[7]

28. A WAP device could therefore be located for tax jurisdictional purposes using the IP address of the Web server or nearest router through which they access the Web. In this regard it would be similar to a consumer using a computer or interactive TV. Location could alternatively be identified using GPS or other aspects of the mobile unit itself. For example, the US Government has imposed a statutory requirement for all cellular phones to have a mechanism enabling their geographic location to be determined.[8] It is uncertain, however that each of these Internet access devices will have the global locating abilities built into cell phones.

29. The current breed of WAP phones connect to the Internet via a WAP gateway which is essentially hard-wired into the phone. (Technically literate WAP users can change the configuration by changing the IP address in the phone, but most users will generally use the default). Therefore, from wherever a user connects to the Internet, they will always connect to the same gateway (even though they connect locally for the pstn access). This gateway will usually be located in the jurisdiction of the service provider, so could be used as a basis for jurisdictional location of the customer). Depending on the information available to the retailer they be able to identify, via the IP address, which WAP gateway any particular WAP transaction goes through.

30. In light of the space constraints of WAP enabled screens, many services are likewise provided through portals or gateways. Tracking of phone based commerce is likely to be from the gateway on to consumer side to the gateway on the supplier side. The current implementation are predicated on local gateways, the location of these gateways in the future may be less geographically specific and may pose greater problems in tracing such transactions to useful locations.

31. The entire promise of ubiquitous or pervasive computing is the ability to access the net from anywhere on any terminal/appliance. It is a non-PC-centric view of the future which places greater emphasis on the use of mobile appliances that are only now being developed to take advantage of emerging protocols. While much has been made of global portability of telephone numbers, it is unclear that each of these Internet access appliances will maintain a fixed IP address. Fixed IP addresses may increase the potential for compromise of security. Even some "always on" technologies (cable, DSL) rotate IP addresses.

Tax rates and classification

32. Once the tax jurisdiction and status of the purchaser is determined, the rate of tax for that jurisdiction must be determined. This rate is often dependent on subtle classifications in the domestic tax code. For many of the intangibles mentioned there is no international consensus as to classification and treatment. Clearly, these are issues which need to be addressed prior to designing any database solution.

33. One concept is for the tax authorities to maintain an approved database[9] of classification and rates that could be relied on by the vendor to compute the liability. Although the technology exists to make such

7. For more information, see the "Wireless Application Protocol Architecture Specification" available at www1.wapforum.ogr/tech/documents/SPEC-WAPArch-19980430.pdf.

8. This location determination ability is also being used by location determination businesses to provide services such as the provision of maps for the consumer's current location and advertising for businesses located within a close range of where the consumer currently is. For example, see www.geeps.com.

9. Please refer to Annex XVII for a more in depth review of Database issues.

a database available, building the database would be a massive job to compile and maintain on a worldwide basis. Existing classification systems might be used as a starting point for goods.

34. For example, the World Customs Organisation publishes a Harmonised Tariff, in which all goods (not services) are capable of being classified for customs purposes under thousands of six-digit categories. The Harmonised Tariff is designed to ensure that a particular good is classified under the same Tariff item regardless of the country of export and import. Each country attaches *its* duty rates to the six digit numbers and, like VAT rates, the duty rates can and do vary by country. Most of the more than 150 major trading nations use the Harmonised Tariff as the basis for applying customs duties to imports.

35. The Harmonised Tariff does not classify services and intangibles. In addition, some rationalisation or simplification of tax categories for goods would have to take place, as the Harmonised Tariff distinctions between six-digit categories are not detailed enough to pick up all of the nuances of the tax distinctions. Simplification of tax classification is an ABSOLUTE PREREQUISITE to enable taxation.

36. A much more practical approach would be to build and maintain a database to describe only digital goods and services. This would be much simpler to compile. The database would be made available on the Internet. An XML standard could be developed so that the database and various commerce applications could communicate and facilitate the tax and duty calculations.

37. For an example of a sample XML classification, see http://tax.dkl.com/xml1.htm, which shows the kind of communication that might take place based on a paper presented by Data Kinetics Limited to the Advisory Commission on Electronic Commerce.

Developments to watch in related fields

38. Exploration into the level of identification is being reviewed as part of the response to recent denial of service attacks and virus attacks. Some governments (US, Justice Dept.) have suggested the maintenance of trace files for a period of time (Three months) an approach which will create nearly impossible burdens on some businesses business (brokerage gets millions of hits a day, and already maintains massive records, maintaining traceroutes for each communication seems like an unreasonable burden. There are other suggestions of a government gateway (EU) which is untenable from the perspective of freedom from unnecessary governmental intrusion. While neither of these options is likely to be viable these discussions will continue to explore the potential to get better information on origination of messages and better ability to identify individuals.

What Technologies are e-businesses using?

39. Another aspect the Technology TAG examined was the approaches that e-businesses are currently using (or may use in the future) to identify the location of their consumers.

40. In general, e-businesses do not have a business need to restrict downloads on jurisdictional needs. Many businesses are interested in their consumers' jurisdiction for marketing and promotional purposes but this information is generally requested directly from the consumer and is not independently verified.

41. Some businesses do restrict downloads based on either individual business or industry needs and in some instances it is a requirement of law. IBM for example only provides downloads from its US based website. These downloads are restricted to consumers who tender a US issued credit card and have a US address.

42. Similarly, Sony music[10] has restricted the sale of both physical CDs and digital music downloads from their US web site to US citizens. They restrict sales by requiring potential customers supply the following mandatory details on registration; a credit card, the US billing address for the credit card, US delivery address and email and other contact details.

43. On an industry level the driver may be protection of copyright. A primary example is the coding inherent in DVDs which split the world into zones with titles released which can only be played on players sold in that zone. On the Internet this driver seems to have most application to businesses that only have distribution rights over products for a particular country. eMusic for example limits distribution of its legal MP3 files to consumers within the USA.

44. However the use of jurisdictional limitations to protect rights on the Internet is not the dominant model. Other mechanisms are instead relied upon to protect rights. For example, Xerox's Digital Property Rights Language (DPRL) is intended to support commerce in digital works using XML:

45. DPRL is used to specify fees, terms and conditions governing the use of digital content. DPRL is extremely flexible and supports multiple business models and rights protection policies, giving publishers the flexibility they need for their current and future businesses. DPRL supports multiple pricing models: subscription-based, outright purchase, purchase of individual rights (view, print, copy, edit, etc.), metered usage, time-based usage, and membership pricing. DPRL defines syntax for specifying rights for a digital document. Rights such as "play," "print," "copy," "edit," etc. can be grouped into named "rights groups"[11]

46. Internet gambling appears to be the primary example of where business restricts downloads or website access based on jurisdictional criteria to comply with government requirements. Until recently, limitations were placed on the export of high levels of cryptography.

47. However the level of jurisdictional verification varies widely and in many instances it is easily avoided through lenient registration processes or by making a false declaration. Where the jurisdictional verification is strong it appears that businesses use traditional processes rather than technological solutions. For example, Lasseter's casino in Australia is required to restrict access to Australian residents of the various states under the current terms of its licence. The registration process at Lasseter's requires player's to provide bank account details, postal and residential addresses, contact details including email and photo identification, passport or motor vehicle licence. In verifying the bona fides of Australian residents, the casino has access to a number of information data bases, such as motor vehicle registration and drivers licence.

48. Another avenue that we explored was the controls over exports of software which included restrictions due to cryptography components. The experience of US based cryptography exporters in using IP numbers to verify purchasers' country in order to meet Bureau of Export Exchange requirements is that a 60 to 70% matching of IP address with the self-declaration was achieved. Note that a mismatch did not have any consequences for potential purchasers more reliance was placed on checks against a denied parties' access list.

---

10. Note: Sony music have structured their Internet presence geographically as opposed to a singular global presence. Not all of their geographic sites offer a Sony internet shop and only the US site offers pay for downloads. Where commercial transactions are possible within the geographic region, the site requires similar registration details as those required by the United States site mentioned above.

11. Cover, Robin; ***The XML Cover Pages*** *Digital Property Rights Language (DPRL)*; 1 May 2000; available at: http://www.oasis-open.org/cover/dprl.html

What technology could be used in the future?

49. There is general agreement that digital certificates and digital signatures[12] show the most promise for identification of parties in the future. Digital certificates (also known as electronic credentials or digital IDs) are digital documents attesting to the binding of a public key to an individual or entity. They allow verification of the claim that a given public key does in fact belong to a given individual or entity.

50. Although the technology exists for digital signatures/certificates and could be very useful in applying tax, with the exception of commerce servers (described below), they are not in widespread use today.

51. In a recent survey of the Global 2,500, Forrester Research, Inc. found that 98% of the firms surveyed employ user names and passwords as their primary means to authenticate consumers, partners, and employees. However, within two years, 56% of these firms see digital certificates as becoming the primary method of authentication, particularly in business-to-business transactions. Forrester notes "interoperability concerns and the sheer number of options deter deployments," and that the proposed X.509 certificate-based Public Key Infrastructure (PKI) standard promises certificate interoperability, but is not yet ratified (see http://www.ietf.org/html.charters/pkix-charter.html).

52. The EU E-signature directive of earlier this year, the current work of UNCITRAL and various other national and local initiatives are part of the flurry of legislation surrounding PKI. Despite all of the legislative activity and technological promise of this technology, however there seems to be little chance of widespread or uniform dispersion of the technology at a consumer level in the next two years. Early adopters of the technology are likely to be governmental or commercial players. The first consumer adopters are likely to be involved in high value/high security transactions. These transactions will likely be related to the financial services sector (banking, brokerage, insurance, real estate) and may include certain high security governmental services. It is unlikely that any of these applications will be those contemplated that require external verification since they will all likely have auditable indicia of the transaction.

53. Issues of cost and technological overhead also complicate, and possibly retard, the speed diffusion. The cryptography and data inherent in a digital signature add complexity and cost to transactions. Part of the delays which SET (Secure Electronic Transaction - digital signature-based security standard developed for credit card transfers) has faced in rolling out are delays in the electronic wallet which result in part from the greater technological overhead. Lastly, the current diffusion of passwords coupled with SSL connections and selective encryption (encrypting only the credit card) have provided an acceptable levels of security for the current types of consumer transactions taking place over the Internet. While consumers may not see an independent need for digital signatures to make small purchases over the Net, they may be likely to use the technology for all transactions once they have it in place for financial or other high security transactions. To assure a critical mass uptake at the consumer level in the mid-term, digital signatures will have to be seamlessly configured in either the browser or the applications.

54. **How do they work?:** Digital certificates go hand in hand with digital signatures. Digital signatures work on key pairs, one of which is public and the other private. The private key is used to encrypt a document while the public key is used to decipher it. The private key needs to be protected to preserve its value. The private key can be stored in various ways. For example, it can be stored on the user's hard disk, on removable media (such as a floppy disk), or on a smart card or other "smart device." These digital signatures are usually used with digital certificates to authenticate the attestation in a

12. A more detailed tutorial of digital signatures is available from the American Bar Association's Digital Signature Guidelines Tutorial "How Digital Signature Technology Works" at http://www.abanet.org/scitech/ec/isc/dsg-tutorial.html

certificate. They could also be used to digitally sign a VAT invoice so that a business purchaser has an electronic invoice that could form the basis of claiming an input tax credit for VAT paid.

55. Digital certificates are issued and managed by Certificate Authorities. A Certificate Authority (CA) is a trusted third-party organisation or company that guarantees that the individuals or organisations granted these unique certificates are, in fact, who they claim to be. CAs can be governments, or private organisations that may or may not be regulated by government. CA functions are no longer necessarily unified; models relating to authentication have begun to evolve dramatically. Previously, all authentication service aspects of the transaction were conducted by one party - the CA for digital signatures. Since then, the functions related to authentication and the types of parties involved and roles they may play have changed dramatically (registration, operation, device creation, …).

56. **Server certificates:** Digital certificates are used today on commerce servers. These server IDs allow web sites to identify themselves to users and to encrypt transactions with their visitors. A CA (e.g., Verisign) issues such certificates for a particular Internet host name (e.g., OECD.org). This kind of digital certificate helps the host server's users know that they are communicating with a particular host and not an imposter.

57. Digital certificates are also used to implement Secure Sockets Layer (SSL), which is the most common form of providing a secure channel between a web browser and the host. Information passing between the browser and the host is encrypted after a certificate sent from the host to the browser is authenticated. Many have come to consider browser-based authentication (browsers have the capacity to hold digital signatures and authenticate the two ends of a communication) to be the largest deployable, scalable authentication mechanism for low value transactions.

58. Unfortunately for tax and reporting purposes the current implementation is only used to authenticate the originating server. This tries to assure the consumer that the business is authentic. There are very few consumers who have the certificate enabled on their browser for a reciprocal check and very few (if any) businesses that require such a check to transact business. There seems to be a business rationale that fraud remains a lower percentage of business and an acceptable risk when weighed against increasing complexity to the consumer. With competition only one click away, the increased complexity or set up/infrastructure requirements drives potential consumers away from a site to the competition. Again, if a higher security/sensitivity (medical, financial, privacy, etc) reason exists for having a certificate in a browser, it is likely that consumers will use it in all transactions.

59. **Using Digital Certificates to Distinguish Consumers and Businesses:** The distinction between consumers and business is not something inherent to Internet technology. This means that the distinction online will only be achieved through the introduction of an identifier. Digital certificates are worthy of investigation as having the potential to deliver this feature. It should be noted, however, that in some legal systems, only natural persons may hold certificates and the person in their corporate function may only be distinguishable from the private person through the use of an attribute field.

60. For example, lets say the revenue authority in a country, or a trusted third party, certifies businesses as being registered in a particular country or countries for VAT purposes by issuing them digital certificates. [13] If the purchaser presents a digital certificate, the transaction would be relieved from tax. If the purchaser does not present a digital certificate, it would be treated as a consumer, and VAT would

13. While this example uses a government issued certificate, there are many national and business models which rely on private sector issues certificates. In some cases government sanctioned accreditation methods are in place, in others agencies my specify objective requirements which certificates used must meet.

apply using the identification techniques discussed previously. Unfortunately, in the area of intangibles a significant minority of the initial on line consumers may be "cutting edge" and may have either level 1 Verisign or PGP certificates.

61. The very nature of authentication as relating to an individual has come into question. Authentication technologies such as digital signatures may be used to identify machines or may be used to establish communications. The underlying information in these uses may not provide the required additional information needed to establish identity. One should also recognise that in some countries, Germany for example, only natural persons may hold certificates, further limiting the potential for digital signatures to differentiate between business and individual users. We must also beware of the holy grail of authentication or identification as being related to the individual. In the majority of cases for the developing models, the authentication may be to a device, which may or may not be under the exclusive control of one owner.

62. Digital certificates clearly show the greatest promise for helping businesses and tax authorities identify parties to a transaction. But the use, character, reliability and deployment of these technologies will vary in the early stages. Tax authorities must understand the technology and its implications to determine the extent to which it can rely on particular implementations.

63. **Revenue Authorities Role**: Revenue authorities need to work with digital certificate providers to increase acceptance and reliability of digital certificates. Revenue authorities must also recognise that government mandated uses of digital signatures have been rejected in favour of accreditation and mutual recognition approaches that specify market-based, objective criteria that provide for proper information verification and technology assurance. Government, industry and users must work together to establish these criteria. The more uses which can be found for digital certificates, such as to insure privacy, enhance security, reduce fraud, the greater the chance that such certificates will gain widespread use. Governments and the private sector must also reach agreement on market based methods of accepting certificates across borders, which would include the procedures for including taxation registration numbers in certificates, where those attribute fields are available.

Future technologies

64. It will also be necessary to continue monitoring the development of future technologies and their impact on both electronic commerce and the taxation system.

65. A recent example is the moves towards convergence of the Domain Name System with the telephone system. One aspect which may prove relevant is a trend towards the convergence of telephone networks and the Internet. The IETF released a Request for Comments RFC 2916 "E.164 number and DNS'[14] dated September 2000 together with an informational draft titled "Administrative Requirements for Deployment of ENUM in North America"[15].

66. The E.164 number is the full international phone number of a subscriber i.e. including country code. The Internet Draft proposes a methodology which would allow transformation of E.164 numbers into DNS names. The following diagram succinctly explains the proposal[16]:

14. Available at: ftp://ftp.isi.edu/in-notes/rfc2916.txt

15. Available at: http://search.ietf.org/internet-drafts/draft-pfautz-na-enum-01.txt

16. Duffy Marsden, Carolyn; *IETF Spec Could Propel Internet Telephony*; 10 February 2000; available at http://www.nwfusion.com/news/2000/1002enum.html

67. The major limitation of the proposal from a jurisdictional verification perspective seems to be that it intends relying on self registration and that there will be a registration cost.

68. Telephone numbers are a potentially good verification data source as they are based on a standard that results in each number being internationally unique[17]. The country code level of the number easily provides the information required for jurisdictional verification. It could be expected that within the next two years, this technology may provide another technological solution.

69. Other moves in the telephone market also point to an internationalisation of their products. For example, British Telecom's GeoVerse™ provides subscribers with a single number for incoming and outgoing calls, voice mail, faxes and emails, plus international Internet access.[18] This single number is currently supported in 71 countries with carriers who recognise the 882 10 GeoVerse™ international code.

70. While this product will initially be targeted and attractive to the business traveller and e-commerce purchases using these numbers may be negligible, it is a direction that will be worth monitoring.

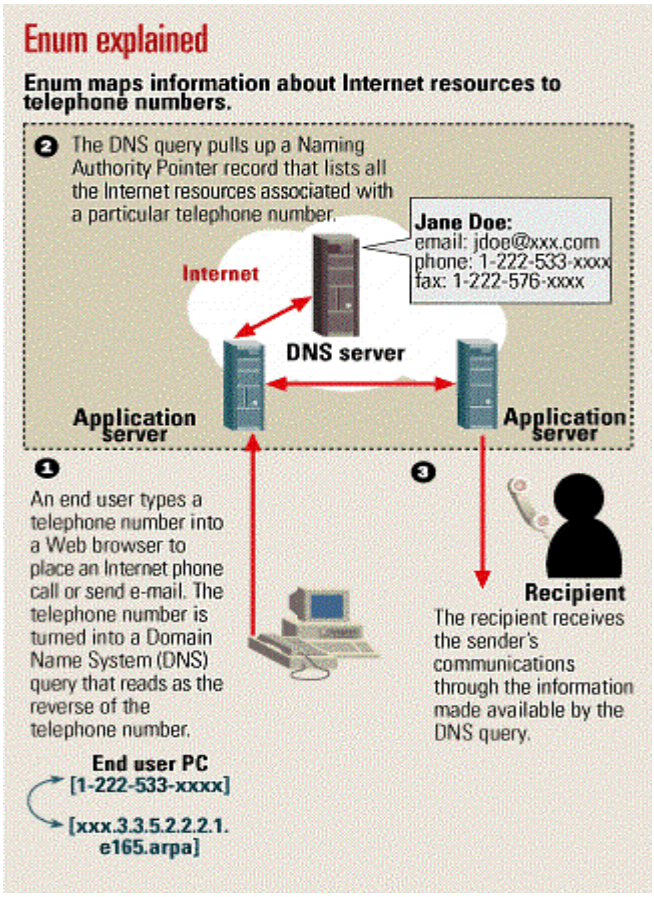
71. The final sub-issue raised here is re the distinction between consumers and business. This is not a factor that is readily apparent to a merchant on the Internet. The nature of the consumer is likely to be identified by their quotation of a reference number (such as the Australian Business Number or local equivalents) or the tendering of a digital certificate which incorporates such information. While this information would normally be acceptable evidence that the merchant was dealing with a business, the lack of such information would not necessarily indicate that the customer was not a business. The reliability of this non-quotation of a business registration number could be expected to be lower where the costs to the business were also reduced by a non-quotation.

Conclusion

72. There is no single piece of information that is either uniformly available or sufficiently reliable to form the basis of a verifiable audit structure. The approach of Digital Island may provide tax authorities with their best option going forward. Digital Island through TraceWare serves as an aggregator and processor of information from multiple sources. Tax authorities are similarly situated at such a point. If this notion is acceptable, our process going forward would be to identify those data elements which could be provided to tax authorities and review those methods by which those elements might be correlated. The banking method of reviewing authentication technologies for ATM deployment is also instructive going forward. The emphasis on these systems was verifying identity, not establishing identity. Using face or fingerprint recognition was only time effective after the customer first identified themselves (usually by providing name and PIN) . Likewise, tax authorities may wish to focus on verifying consumer or business declarations not establishing them outside of such a declaration.

17. This system is under the auspices of the International Telecommunication Union (www.itu.int).

18. See www.geoverse.com


Enum explained
Enum maps information about Internet resources to telephone numbers.
2 The DNS query pulls up a Naming Authority Pointer record that lists all the Internet resources associated with a particular telephone number.
Jane Doe:
email: jdoe@xxx.com
phone: 1-222-533-xxxx
fax: 1-222-576-xxxx
Internet
DNS server
Application server
Application server
1
An end user types a telephone number into a Web browser to place an Internet phone call or send e-mail. The telephone number is turned into a Domain Name System (DNS) query that reads as the reverse of the telephone number.
End user PC
[1-222-533-xxxx]
[xxx.3.3.5.2.2.2.1.e165.arpa]
3
Recipient
The recipient receives the sender's communications through the information made available by the DNS query.

ANNEX V:
CREDIT CARDS AND CONSUMERS' JURISDICTION

Introduction

1. The Technology TAG has explored various options for verifying the jurisdiction of consumers who purchase digitised goods over the Internet in order to properly impose consumption taxes. In particular, the Technology TAG has explored whether credit cards[1] currently provide the information necessary to verify the place in which consumption occurs in business to consumer transactions. Due to the central role of credit cards in on-line payments for consumer transactions, there is a natural proclivity to assume that credit cards can ideally serve as valid indicia for verifying the place of consumption. However, there are severe commercial limitations which make credit cards not viable for this purpose. In addition, the use of credit card numbers or an issuing institution's identification numbers as a proxy for jurisdiction does not appear to be a workable solution. Our findings and comments herein are made after consultation with several major global card issuers, card associations, and industry groups.[2] The limitations associated with these proposals are discussed below in full.

Possible use of credit card indicia for verifying the place of consumption

Current and future use of credit cards as a primary mechanism for purchasing items on the Internet

2. While credit cards are currently the dominant method of payment for goods purchased over the Internet, it is important to note that there have been significant developments towards other payment mechanisms, including digital cash and stored value cards. Alternative payment mechanisms such as digital cash and stored value cards are the second-generation payment systems for many Internet accessible jurisdictions around the world. These payment systems are becoming more widely accepted for e-commerce transactions as new and innovative solutions come to the market place. Any proposal to use credit cards as a primary vehicle for verifying the place of consumption assumes that credit cards are and will in the near future be the dominant, if not exclusive, form of payment for consumer transactions over the Internet. The development of alternative payments systems should be monitored by the Technology TAG to see whether a possible verification solution matures, since focusing on only one means of payment could lead to distortions and lack of neutrality by influencing consumers in their choice of a payment method.

3. Whether a transaction is taxable or not and, if so, the determination of the rate at which it is taxable should not depend on whether a specific payment method is being used. Such an approach places the existing credit cards at a great disadvantage and ultimately may push consumers towards using alternative payment schemes, and less accountable means of payment in order to avoid paying consumption taxes. Therefore, the inclination to assume that credit cards are ideal for verifying the place of consumption, simply because credit cards are a method of payment, must recognise the growing development of alternative payment mechanisms.

---

1. This document is intended to cover payment cards in general, including both credit and debit cards.

2. Industry participants included American Express Company, Citigroup, Discover Financial Services, Inc., EuroPay, Household International, MasterCard International, Visa EU, Visa USA.

Credit card billing address as proxy for jurisdiction

4. The Technology TAG explored whether a consumer's credit card billing address could be used as a proxy for jurisdiction in the sale of digital goods over the Internet. At the outset, it must be observed that a credit card billing address does not always represent place of consumption or the place of residence of the consumer. Digitised products may be consumed at locations other than the place where a consumer's credit card bill is mailed. For instance, a consumer may download products from the Internet while he or she is on vacation, on business travel, or on a college campus. Consumers often have their credit card bills sent to their place of employment, post office mailboxes, or other addresses.[3] However, since jurisdiction for consumption taxes would be determined on a country level, presumably the variation in billing addresses should not make a substantial difference. The use of a consumer's address (residence) as the predicate for consumption tax jurisdiction requires further exploration of each business model or other source that use consumer addresses, not only the credit card industry. The future mandate and work plan of the Technology TAG should include inquiry in this area.

5. While a consumer's billing address is contained in the card issuer's business records, the fields of information necessary to verify an address for country level jurisdiction are not accessed at the point-of-authorisation in a credit card purchase. Furthermore, the notion of delving into a credit card issuer's files to access cardholder personal information (such as where that person lives or where his or her bills are sent, in order to disclose such information for a vendor to determine whether the cardholder properly declared his or her place of residence) raises serious concerns of privacy, security, and confidentiality, as well as other legal issues.

The Authorisation Process-Real Time Access

6. When a cardholder uses a credit card to purchase goods or services, the merchant's request for authorisation is electronically transmitted to the card issuer. In certain card systems and transactions, this authorisation process may involve credit card associations. The merchant contacts the card association, not the card issuer, for transaction approval. Card associations like MasterCard or VISA or other networks are intricately involved in transmitting the request for authorisation and communicating the approval or disapproval to the merchant when a credit card is used to pay for a transaction. The authorisation process occurs in real-time communication at the point-of-sale. The systems design and infrastructure for authorisation incorporates fundamental protections relating to privacy, fraud control, and confidentiality. Information transmitted from the card issuer to the merchant, through the cards association, is often limited to approving or declining the transaction based on the cardholder's available line of credit. No personal demographic data is transmitted, only financial data. Access to a cardholder's address is not a part of the normal transaction authorisation process.

7. Changing the authorisation process in order to verify an address for tax purposes would require altering fundamental business policies and protections which could lead to considerable system modifications at significant costs to the credit card industry. These changes would not only affect card issuers and cardholders but they would also require changes in systems for card associations, merchant banks, and other transaction facilitators.

8. Changing the authorisation process would not only delay the authorisation of transactions, but it would also slow down commerce. If the consumer declares an incorrect address, the merchant would not know the correct taxable jurisdiction and therefore would not know the total cost (price plus the

3. American Express forecasts that up to 10% of their US clients will appear to have New Jersey addresses by the end of 2000 as they arrange their bill paying through PayTrust.

appropriate tax) for which approval must be sought. Under the current authorisation procedures, the merchant would need to seek a second authorisation if the original jurisdiction was not verified for the revised amount of the tax. This multiple authorisation process would not only slow down transaction processing, but also lead to an increase in processing costs. The effect of such changes undermines principles of neutrality between digitally delivered goods and physically delivered goods because in a physical goods environment only one authorisation would be required. It must be noted that this is a limitation of current proposals which will need resolution in order not to hamper the development of electronic commerce.

9. An important aspect of maintaining systems integrity from fraud and misuse is to release only so much information to the merchant about a cardholder that is necessary to complete the transaction. Systems modifications, other than those done to serve business goals, compromise a system's integrity.

10. Any proposal that requires a change to the business model of financial institutions in order to obtain the billing address of cardholders at the point of sale for a digital product creates a significant burden on the credit card industry for the small portion of credit card transactions subject to the authorisation process. The vast majority of transactions are for non-digital products, which do not require this data. It is doubtful that such a proposal could ever justify the required investment for a small return.

Privacy, Confidentiality, and Security

11. The biggest barrier to growth in online purchasing is consumers' fears of online credit card fraud, security, and privacy concerns. A customer's expectation that a financial institution will respect the privacy and confidentiality of their business relationship is fundamental to the relationship between an institution and its customer. To the extent that a card issuer provides or verifies personal information, such as a residential address to a merchant or to anyone else for a purpose unrelated to approval or disapproval of the credit card transaction, raises privacy and confidentiality concerns. A cardholder has a reasonable expectation of privacy in the information that it furnishes to card issuers for the purpose of obtaining credit. Privacy protections of cardholders' personal information are contained in privacy laws in the United States, the European Union, and in other major jurisdictions around the world. The privacy provisions differ considerably from country to country, and there are restrictions on transferring personal data from the European Union to other countries. A card issuer's access of its records to obtain personal information about a cardholder in order to disclose or verify such information with a merchant could potentially expose the card issuer to liability.

12. An important component of the card issuer-cardholder relationship is the reassurance given to the cardholder that the institution will safeguard personal information in strict confidence. This confidentiality promise is written into many card agreements and policy statements published on the Internet and elsewhere to inform customers of the institution's policy. Such assurance is essential to customer confidence, particularly in the case of on-line transactions, where customers concerns about privacy are especially acute. Credit card issuers are sensitive to consumer fears about revealing their personal and confidential information over the Internet. The public perception that personal information such as a cardholder's place of residence would be released by financial institutions to online merchants raises industry concerns that this could seriously erode consumer confidence, compromises confidentiality, and could potentially expose them to legal liabilities.

13. The United States Comptroller of the Currency, Administrator of National Banks found that a number of financial institutions have recognised the growing importance of privacy to their customers and

have developed, implemented, and communicated privacy policies.[4] The Comptroller's advisory opinion in discussing effective means of communicating a bank's privacy policies states that…

> "…Many banks that post privacy notices on their Web sites acknowledge their customers' privacy expectations and indicate how the bank will safeguard and handle personal information. In many instances, banks inform their customers that the bank takes measures to limit employee access to confidential information and to maintain accurate and up-to-date consumer records. Some banks also describe the general circumstances under which the bank will share information with third parties. Some banks explain that customers have a choice about how their information is shared and provide a convenient way to "opt out" of mail or telephone solicitations… To ensure that the privacy principles are readily understood, some banks have supplemented these principles with a series of questions and answers about handling customer information."[5]

14. The credit card industry experiences significant exposure for fraud related to unauthorised use of stolen or lost credit cards or counterfeit or altered cards. Online transactions raise particular concerns about fraudulent use of a cardholder's credit card number or a cardholder's repudiation of transactions. Therefore, card issuers limit the amount of information that must be disclosed online about their cardholders in order to protect against such information falling into the wrong hands. Just as the address of a cardholder is viewed as an acceptable means of authentication, a fraudulent cardholder may use that address to legitimise an otherwise detectable fraudulent transaction. For example, if someone steals a consumer's credit card and also knows the consumer's address, the thief can order goods or download digitised products disguised as the true cardholder.

Address Verification System

15. In some parts of North America, merchants can use an Address Verification System ("AVS") to check portions of the address of a cardholder. AVS was developed for the mail-order catalogue industry as a tool to reduce fraudulent use of a cardholder's credit card number. The system allows mail or telephone order companies to compare a portion of the address provided by the customer to the billing address on file with the card issuer in situations where fraud might be suspected. Merchants do not have access to the card issuers file information. The manner in which this comparison is done differs between card issuers, card associations, and operating systems. Some systems involve a portion of the address fields being converted by an algorithm or mathematics formula into a code, which is transmitted to the card issuer or card association. Some merchants communicate the data to a credit agency. The agency processes the data and returns a confidence rating, which could either outright recommend decline of the transaction, could grey score the transaction, or could give a percentage confidence match. Some merchants use commercially acquired AVS systems to check addresses. Ultimately, the decision is left to the merchant as to whether or not to continue with the transaction after attempting to verify the address. The fact is that there is no full address match by the card issuer or card association. In addition, the system is not designed to verify the

---

4. See Office of the Comptroller of the Currency, Advisory Letter 99-6, Guidance to National Banks on Web Site Privacy Statements stating that "A number of banking trade associations – the American Bankers Association, the Consumer Bankers Association, the Banking Industry Technology Secretariat of the Roundtable, American's Community Bankers, and the Independent Community Bankers of America – have adopted a core set of banking industry privacy policies. These industry- wide policies have been used by many banks as a starting point for developing privacy policies tailored to their individual corporate practices." Other countries may have alternative approaches with respect to disclosure of information about customers.

5. id

cardholder's country. It simply confirms or denies a portion of the cardholder's address. The AVS business practice is locally driven, reflecting the development of each system for use within a country rather than on a global basis. The fields used for address verification are not uniform throughout the industry. Some systems might use the house number and street name to verify that the mailing address matches the billing address (*e.g.*, 10 Main Street), while others might use a postal or zip code. In some instances, the AVS may use totally different fields. As previously indicated, however, there is not a country level match.

16. An address verification system will be available in the United Kingdom in 2001, and could become available in other countries, "where the reference data exists" to develop such a system. However, there are no firm plans for such development in other countries for at least 2 years. The card industry has developed its own address verification solutions in the UK, but this typically verifies only the numeric portions of an address, such as the house number and postal code. The result returned is a "score" of probability that the verification is accurate. While it is possible that emerging commercial offerings, in the future, might be able to confirm whether a particular person exists, and that the declared address corresponds to a full registered address, that technology is not part of the existing business model today. The underlying theory that AVS will be further developed assumes that relevant data for the individual-consumer exists in national consumer databases, e.g. is a registered voter, and that the necessary voter and postal data is available for commercial processing.[6]

17. The AVS was designed to deal with concerns that are much different than those relevant in the tax collection context. The AVS is directed at combating fraudulent use of a credit card by determining whether the person in possession of the card is the true owner or an impostor. One way of making such determinations is to ascertain whether such person knows personal information, such as the street address, of the cardholder. Thus, a verification match of "10 Main Street" might be sufficient for this purpose. The proposed proxy for tax verification, on the other hand, is directed at the true owner of the card, who the government suspects will make a false declaration of his or her country of residence in order to evade the consumption tax or to obtain a lower consumption tax rate. Using the AVS to verify a cardholder's declared residence of "10 Main Street" in "Luxembourg" would facilitate a match of the street address, but it would not verify the cardholder's country of residence if the consumer in fact resides at "10 Main Street" in the "United Kingdom." Therefore, AVS would not only be unreliable for the purpose of determining tax jurisdiction for consumption tax, but could also validate a false declaration.

18. Interestingly, the AVS system has not been as effective in preventing online credit card fraud as in other transactions. AVS is a time consuming process that delays transaction processing. The normal authorisation process is electronically performed primarily to determine whether a cardholder has sufficient buy/credit limit to complete his or her transaction. When this process is encumbered by the need to check addresses, which might involve converting address fields to codes, decoding data, determining confidence levels, transmitting data to credit agencies, etc., billions of daily transactions are affected causing time delay in completion. Consequently, the credit card industry is exploring other fraud prevention tools such as disposable credit cards, anonymous card numbers, fraud screening devices, up-to-date security systems, encryption, electronic codes, passwords and more secure on-line environment, etc.

19. Further difficulty arises from the fact that the authorisation process is not uniform among payment systems. There are different systems and operational practices used by card associations, card issuers, and networks. Furthermore, because there are significant differences in the layout of addresses, it will be difficult to use one AVS system for cross-cross-border verification purposes. Also, a consumer's address is changeable at the consumer request to suit his or her convenience. Adapting the system to

6. Card industry representatives have had discussions with Equifax and Experian. These companies are engaged in the business of developing address verification systems.

accommodate such differences will not only be time consuming, but costly. If Internet transaction processing is slowed down then consumers are more likely to become frustrated and not complete the transaction. When a merchant must scroll through an address listing or input address data into a system or convert an address by an algorithm into a code which must be transmitted, decoded, encode and re-transmitted, or transmit data through a credit agency, all so that he can match a consumer declared address, which might not match for various reasons unrelated to a false declaration, this could lead to an appreciably decelerated process for a merchant processing thousands or millions of transactions.

Credit card numbers or issuing institution's identification number as proxy for jurisdiction

20. The Technology TAG explored whether the account number on the face of a consumer's credit card or the identification number of the card issuing institution, commonly referred to as the Bank Identification Number (hereinafter called the "BIN"), could serve as a reasonable proxy for jurisdiction of the place of residence of the customer in the sale of digital goods over the Internet. BINs are used to identify the issuer of a specific card. They also identify the settlement, billing and authorisation currency used by a particular bank. For reasons stated below, neither the card account number proposal or the BIN proposal is a workable solution.

Card Numbering System

21. Each credit card contains a range of numbers. The numbering system is designed for identification and security reasons peculiar to the card industry. The numbering system varies by card associations and card issuer. The range of digits consisting of six fields generally denotes the type of credit card or card association and the issuer. The numbers also correspond to the internal coding system of the card association and/or card issuer. Other significant digits on the credit card correspond to a randomly assigned cardholder's account number. The card numbering systems do not identify the country of residence of the cardholder.

International Standards Organisation Registry

22. The Technology TAG explored using a registry centrally controlled by the International Standards Organisation (hereinafter "ISO") to determine the country of location of a card issuer. The ISO is a voluntary organisation in which card issuers may choose to participate. This proposal involved using the country where the credit card issuer is located as a proxy for place of residence of its cardholder. Using the ISO registry as a data base, the merchant would look up the location of the card issuer corresponding to the BIN shown on the credit card presented by the cardholder and then cross check that location shown in the registry to the place of residence declared by the cardholder. This hypothesis assumes that the cardholder resides in the country where the card issuer is located, an assumption that is often incorrect.

23. After considerable review, the Technology TAG concluded that the ISO registry is not a reliable source for determining country of location of the card issuer. Moreover, the ISO registry does not identify many of the larger card issuers and the most widely used international payment cards. The registry merely identifies the card associations against a range of BINs. The address shown for the major card associations is the United States. As to some card issuers identified in the registry, the address information relates to their headquarters in the United States, and is outdated. The ISO registry does not identify each card issuer by name, address, city, state, postal code and country against the card issuer's BIN.

24. BINs were not developed or intended for identifying cardholders' place of residence, and they are not used for such purpose by the credit card industry. Moreover, the location of the credit card issuer as a

proxy for place of residence of the cardholder is not reliable for several reasons involving mobility of cardholders, cross-border card issuance, changing business environment, and alternative payment systems. In addition to the inherent limitations in existing business models, the European Union movement towards an internal market for financial services makes BINs associated with a particular country less reliable as indicia of a consumer's place of residence. [7] While the EU internal market for financial services may still be in its infancy, cross border issuance is already a reality.

Mobility of Cardholders and Cross Border Issuance of Credit Cards

25. The assumption that a cardholder resides in the country where the card issuer is located is not valid where a cardholder moves for business or personal reasons. It is not unusual for a cardholder to reside in a country other than the country where the card issuer is located. Cardholders often change residence without changing their business relationships with their financial institution. Such cardholders would maintain their credit cards with the card issuer located in the jurisdiction of their former residence.

26. In some border regions, consumers tend to shop cross-border for payment cards to take advantage of lower fees, reward programs, and other benefits. With the growth and development of e-commerce and Internet banking, access to services attendant to a payment card and competitiveness in the industry may lead to more cardholders holding credit cards issued in several different countries. Furthermore, associating a particular payment card or BIN with consumption tax, or higher costs, could increase consumer demand for cards issued in jurisdictions not associated with such increased costs. In these or similar situations, the BIN of the card issuer would not correspond to the cardholder's place of residence or place of consumption.

27. Banks already do cross-border issuing of payment cards from their country of establishment into other markets and are expected to increase these activities. In such an instance, the BIN used for cross-border issuance may also be used for domestic issuance. Within the next year, several new forms of multi-currency and multi-country issuance of payment cards under a single BIN are expected to become a reality. The BIN used would still serve to identify the issuer; however, the cardholders will be located in several different countries.

Changing Business Environment

28. The BIN may be used to identify settlement, billing and authorisation currency used by an issuing institution. While certain digits included in the BINs relate to currency, there is no consistency within a card system or between card systems. The placement of the currency digits, the numbering system, and what the digits mean vary by card associations and also vary within certain associations. Many of the cards systems do not identify a billing, settlement, or any currency characteristics in the card numbering system. Some BINs identify the settlement currency between the acquirer and the card issuer. In some card systems, depending on when the card was issued, the BIN might identify the billing currency. There is no business need for consistency between card systems. The merchant only needs the transaction currency, which he knows up front. Furthermore, most card issuers settle in *US* dollar today. With a single European currency almost fully implemented, the use of separate country designated BINs in the European Union will be less important since the currency distinctions will no longer be necessary. The business model could gravitate toward a single BIN for the euro.

---

7. The EU moves towards a single market for collection of VAT on digital downloads may mean that this is not a limitation within the member countries. However similar moves to centralise card issuance may occur amongst other countries.

29. New credit card products are being developed to respond to business and consumer concerns about online fraud. These new payment systems could lead to obsolescence of BINs as they presently exist. For instance, American Express recently announced that it is moving toward disposable numbers using a random numbering system.[8] Without the credit card number at the point of sale, utilisation of the BIN to identify location of the issuer will be even more difficult. Single use disposable numbers will have a BIN that simply means "3rd Party Single Use Disposable". They will not even indicate the continent of the card issuer. So even though the BIN format exists for ISO purposes, it could not work as a proxy for real time transactions. Consumer demand will dictate the speed in which these products become prevalent. A consumer survey conducted by the Gartner Group in 1999 indicated that 87 percent of respondents were "very concerned" about sharing their credit card information online. When Internet users who do not shop online were asked why they do not shop, an equal number said they either saw no value in buying online or they did not want to disclose financial information.[9] Orbiscom first launched its wallet with Allied Irish Banks in August. In two months of use, ten percent of Allied Irish's active Internet banking customers who had credit card accounts downloaded the software.[10]

30. Financial institutions are now offering customers a wide range of new payment capabilities that will transform how consumers make payments over the Internet. Consumers will now have more choice with a variety of online payment options including money transfer, lines of credit for Internet transactions, and other payment features. Some of these payment mechanisms might not involve institutions with identifiable BINs, or might involve institutions that operate on a global basis, making it very difficult to rely on a BIN system as a proxy for any particular jurisdiction.

Conclusion

31. The work of the Technology TAG with the credit card industry has led us to the conclusion that credit card information is not viable as a means of either verifying a consumer's place of consumption or as a proxy for establishing a consumer's jurisdiction. The industry's business models and the technology underlying credit cards were designed to meet needs that have resulted in their not being suitable to provide merchants with the information they would need to verify a consumer's jurisdiction.

32. The Technology TAG appreciates the input and expertise made available by the credit card industry in undertaking this review. The TAG proposes to maintain the good working relationships developed with the industry through this process to ensure that each is kept current on developments in each other's fields of expertise.

---

8. American Express Credit Cards to Offer Disposable Numbers for Web Shopping By Jathon Sapsford, Staff Reporter of THE WALL STREET JOURNAL. The card number would be good for one transaction only, and shoppers would no longer have to give their credit-card number to merchants over the Web. jathon.sapsford@wsj.com

9. A survey commissioned by Intelishield.com Inc., a Denver-based disposable card software developer came up with similar results.

10. Disposable Nos: Flaws Catch Up With Hype by Lavonne Kuykendall, American Banker, October 26, 2000.

ANNEX VI:
TECHNOLOGY AND PLACE OF CONSUMPTION

What impact does the WP9 Sub-group's guideline that "place of consumption" equates to the "consumer's permanent address, or alternatively, their usual place of residence" have on our recommendations / findings? How can technology support this guideline?

1. The proposed guideline creates challenges for any verification technology that dynamically determines a consumer's current physical location or jurisdiction. The major example is the proposed use of IP address tracing technology.

2. Traceroute, or similar utilities, determine the location of the consumer's access point to the Internet subject to the technological limitations outlined in Annex IV. Due to the cost of long distance phone calls, this will generally be through an ISP server located geographically close to their physical presence. So IP address traces may provide a some verification of the jurisdiction of the consumer's current location. Given the use of "roaming" utilities and "Internet cafes" to gain Internet access through a local portal anywhere in the world, this technology has no reliable relationship with the consumer's permanent address or usual place of residence.

3. To support this guideline, a lookup would be required to some more permanent or static source of information that includes the consumer's normal country of residence. Perhaps the best way of achieving this is through the consumer providing this information through a trusted source. This leads back to the need for consumers to provide this information through a digital certificate, perhaps stored on a smart card to aid portability and provide security over the certificate. However as stated in the original paper, this technology is not yet in common use by consumers, isn't required by current business models and those digital certificates that are currently being issued to consumers are generally lacking the rigorous verification of source information that would be required by revenue authorities.

4. As discussed in Annex V, further research with the credit card companies is indicating that the use of their information databases or the credit card numbers themselves are unlikely to provide a viable solution to our jurisdictional verification challenges. The solution based around the current credit card driven business model that may however have some potential is the use of Address Verification Systems (AVS).

5. At present AVS is only available in the USA. However they are planned to be used in the UK from April 2001 and are expected to be extended to other countries. Rather than being a shared product, each credit card company has developed their own AVS. They advise that there is a convergence in their use of AVS although they get there in different ways. Credit card companies do not believe that AVS is an appropriate vehicle for consumer identification for revenue purposes.

6. AVS is essentially a fraud prevention tool. Basically the merchant gets the consumer's mailing address and checks this against residence details in the AVS to see if the given address is likely to be accurate. It only matches elements of the address *e.g.* AMEX uses the postal code and the street address. So the merchant doesn't appear to get access to the consumer's complete address.

7. It also doesn't currently extend to country verification as each version of AVS has been developed for use within a specific country rather than for international usage. It is likely that as cross border card issuing becomes more prevalent, the various AVS systems will have to be expanded or get more systematic. If the market is left to do this development without input from revenue or other authorities, it can be expected that each company will continue to develop their own systems as the companies currently maintain their own systems for security, proprietary, privacy and other business reasons. Each companies' AVS is developed to fit with their own business model.

8. An option may be for revenue authorities to have input into the development of AVS or start work on their own guidelines on what an AVS should include to meet merchants' taxation obligations. An interesting corollary can be drawn with the database proposed in the US under the provisions of the *Mobile Telecommunications Sourcing Act*:

> "The bill would determine taxes based on a subscriber's billing address as opposed to where a call originates, is switched or relayed.
> …
> Under the bill, states can create electronic databases that designate the appropriate tax jurisdiction and tax-jurisdiction code for each street address in the state. Both the Federation of Tax Administrators and the Multistate Tax Commission, organisations that represent state and local tax officials, must approve the electronic database system. If a state chooses not to develop a database, service providers can develop their own databases based on an enhanced ZIP code, also known as a ZIP+4 code. Any provider would not be liable for an erroneous tax or charge that was assessed due to an error in the state-sanctioned database or its own proprietary database, as long as it was created after exercising due diligence.
> …
> A more accurate solution, as supported in the Mobile Telecommunications Act, is to assign tax-jurisdiction information to 9-digit ZIP records. This approach assigns Census geocodes to each customer-address record. The enhanced ZIP code corresponds to a city block or street segment, and typically only one side of a street, which is an important functionality because tax-jurisdiction boundaries may differ on the same street. The returned geocodes can then be cross-referenced to the corresponding tax rates for that location."[1]

9. It should also be noted that the credit card companies are moving from AVS towards other fraud control devices. This includes the "single use" credit card numbers recently introduced by Amex as discussed in Annex V. This may mean that greater potential lies with independent commercially available AVS which can be developed to meet our specific needs rather than linking into a model that businesses are moving away from. In addition to continuing to explore these options with the card companies, the Technology TAG has initiated contact with some commercial AVS developers.

10. We would like to conclude with some overall comments on the proposal to equate place of consumption with a permanent address rather than the place where the consumer is. The proposal is basically one that doesn't fit with any of the directions that technology is heading in. The technological solutions are ones that are more "real time". That is they are based on what is happening now which includes the current jurisdiction of the consumer. The only exception is the potential usage of digital certificates to store such knowledge. This has severe limitations at this point in time as discussed above and in Issue 5 below.

---

1. Peikin, David; *The Final Tax Tally*; 15 April 2000; available at http://www.wirelessreview.com/issues/2000/00415/feat21.htm

11. In the view of the Technology TAG, it will prove easier to collect consumption taxes based on the jurisdiction of where the consumer is. Another example of this is the expected growth in use of mobile phones for e-commerce which again are easier traced through real time mechanisms if current technology is to be relied upon.

12. While permanent address may have value as a throwback rule, we would counsel against its adoption as the primary measure of place of consumption.

ANNEX VII:
SELF ASSESSMENT AT PLACE OF CONSUMPTION

Overview

1. Per the Working Party No. 9 Sub-group on Electronic Commerce paper entitled, *Electronic Commerce—Tax Collection Mechanisms* (WP9 Sub-group Paper or "Paper")[1] - under a self-assessment at place of consumption system, recipients would be required to determine the tax owing on imports of services and intangible property, and to remit this amount to the domestic tax authority. The self-assessment collection system is considered separately for Business-to-Business trading and Business-to-Consumer trading.

Business to business

2. Per the above-mentioned Paper - the self-assessment system is feasible, and in fact exists in most jurisdictions for cross-border business-to-business transactions. In addition, the self-assessment system is effective. Effectiveness of this system for business-to-business transactions is due firstly to the fact that the receiving business falls within the audit reach of Tax authorities and secondly that the cost of VAT or Sales Tax can be written off against their tax liability. No technology issues have been identified with respect to either tax authority administration support nor tax authority compliance support.

3. All businesses will have existing consumption tax administrative and compliance procedures in place. The self-assessment model will place no significant additional burden on business. Unfortunately, not all countries have business "self assessment" or reverse charge provisions, and such rules would need to be enacted in those countries who wish to tax imported services or "virtual products". There are, however, issues of enforcement across VAT and non-VAT systems and the ability to recover or properly assess and remit VAT. Business administration and compliance is currently predicated on national rules and systems of taxation. As more transactions become international and as more SMEs enter the market, greater problems could arise. Developing a global database to facilitate tax calculation could enhance compliance in these situations[2].

4. The provision of customer service support for electronic filing and electronic payment of liability is not directly relevant to the administration of the Self-Assessment collection mechanism issues under debate. However, ease of use, calculation, administration and remittance would be great incentives for compliance at the business to business level[3]. Electronic filing and electronic payment services have the potential to reduce compliance administration costs and complexity and therefore may increase the rate of

---

1 . This paper, to which the present document refers was a working draft shared with the Consumption Tax TAG but not made publicly available. The salient features of the paper, however, feature in the Working Party No. 9 Report to the Committee on Fiscal Affairs.

2. See Annex XI which provides an overview of the benefits, architecture and maintenance issues involved in developing such a database solution.

3. Please see Annex XIV which provides an overview of development and implementation issues related to electronic filing.

compliance. This information is also required to address the alleviation of the supplier compliance burden under the Registration collection option addressed below.

5. In order to ensure the access of the technology solutions, the policies and procedures related to collection mechanisms would also need to be clarified. For example, will these assessments result in annual or transaction disclosures. Will SMEs have trouble with the identification of and remittance to the appropriate authority? A number of these factors are common to the other approaches and may need to be addressed as part of any overall solution.

6. The WP9 Sub-group Paper notes that effective mechanisms exist in tax authorities for the enforcement of consumption tax through returns compliance programs and audit programs. These enforcement mechanisms could be expected to apply effectively for these B2B transactions.

Business to consumer

7. The self-assessment system is feasible for business to consumer transactions. However, few jurisdictions operate a self-assessment collection method for Business-to-Consumer transactions. Canada operates self-assessment and US states operate a form of self assessment called "Use Tax". Collection of revenue from use taxes arising in respect of cross border transactions has however proved problematic.

8. The WP9 Sub-group Paper identifies the collection enforcement of VAT on services and intangible property supplied to the consumer as the main problem with the effectiveness of this solution.

9. One alternative is to register consumers and incorporate them into the current VAT/consumption tax collection systems. The following problems have been identified as arising with this solution which would increase consumer compliance burdens.

10. **Firstly**, the success of such a system depend on consumer knowledge. Ordinary consumers generally lack knowledge of which services are taxable, zero-rated, exempt, or subject to a preferential rate, particularly in tax-inclusive VAT systems. At present there is no real technological solution, which presents itself to assist consumers. There are certain mitigating procedures, which can be put into place and certain convenience features which may make compliance more likely. If governments maintain a centralised database of tax reference and classification information, then businesses can more easily develop products which can query the reference tables and provide the consumers with a pre-calculated amount of tax payable. Depending on table organisation and supporting technology, the information provided to the consumer may include the tax authority contact details as well as the potential for an electronic remittance.

11. **Secondly,** consumers will need to keep certain records or accounts. There are plenty of cheap accounting packages available for purchase. There are also simple household accounts and record keeping packages bundled for nothing with some software. In any event the relevant record keeping is quite simple and so could be maintained manually. Questions do arise in terms of transactional versus annual reporting, however. Record keeping can be expected to be problematic with compliance verification by revenue authorities complicated by the number of transactions and collection points to be dealt with.

12. **Thirdly**, consumers would be obliged to make periodic VAT/Consumption tax returns. This issue has more significant implications when applied in the context of sales taxes and VAT and the gulf of understanding and practice existing between the two. The same customer service requirements would be needed here as discussed above for B2B transactions. These customer services are not directly relevant to the administration of the Self-Assessment collection mechanism issues under debate. However, electronic

filing and electronic payment services have the potential to reduce compliance administration costs and complexity and therefore may increase the rate of compliance.[4]

13. In addition to the burdens on consumers, there would be additional burdens on tax authorities and tax administration. The extent to which tax authorities could successfully audit individuals for their purchases of imported services and intangible property under this mechanism is highly uncertain. Specifically, it is doubtful whether tax authorities would have the ability to identify individual purchases of nominal value by consumers. Moreover, it is uncertain whether tax authorities would conclude that it was indeed cost-effective to do so.

14. Any such assessment system would initially require the consumer to disclose his or her jurisdiction which could then be verified (but only to a significant degree and not to a definitive certainty). The verification would be against collateral information, including: delivery address, registration address, billing/payment information or IP address/Domain. All of these factors have limited accuracy and many of them may raise privacy implications. Digital Signatures may at some point be used as part of this solution. Special attribute fields would need to be developed which could correlate jurisdiction as they are not necessarily essential to establishing identity. Issues of what acceptable standards may be applied to accepting these criteria remain in issue. For example, what is an acceptable registration authority? What are the obligations of due diligence? Is there a commercial rationale for this service? Will commercial certificates be acceptable? It is the generally held view of international business and of many governments, that it is the market's role to determine what technology solutions have commercial merit.

15. In addition, there would be an incremental cost of data capture and maintenance. Attempting to capture a large proportion of such transactions under this system could require substantial communications efforts. Questions to be answered include: will these assessments result in annual or transaction disclosures? Will consumers have trouble with the identification of and remittance to the appropriate authority?

16. Issues of cost and likelihood of commercial deployment have also not been properly factored. Different transactions warrant different levels of security and authentication. Mandating a higher than needed level of authentication and investigation in low value transactions makes no commercial sense, places unreasonable amounts of technical overhead and complexity into a transaction and will impair the commercial viability of private sector systems.

4. See the electronic filing and electronic payments Annex XIV.

ANNEX VIII:
REGISTRATION OF NON-RESIDENT SUPPLIERS

Overview

1. As discussed in the WP9 Sub-group Paper (see reference in Annex VII), the Registration model would require non-resident businesses making supplies into a jurisdiction to register in that jurisdiction and charge, collect, and remit consumption tax in that jurisdiction.

2. This option is seen primarily as a mechanism for effectively dealing with the identification and taxation of cross border business-to-consumer transactions. The self-assessment mechanism is generally being favoured currently for the collection of taxes in the case of cross border business-to-business transactions.

3. Application of the self-assessment system would only be permitted for business-to-business transactions after the consumption tax status of the customer had been positively established. Without proper identification, customers would always be deemed private consumers falling under the scope of the registration system. If reliable identification of business customers is not possible, extension of the registration model to all transactions could be considered.

4. At the outset, we must recognise the limitations of a national-based scheme of registration to address the needs of a global medium. Consideration of a global registration system would help address a number of these issues and facilitate registrations for companies with global operations as well as SMEs who have gained access to global markets through the Internet.

5. On first review, extending tax collection obligations to non-residents seems a feasible proposition, as it would involve only the adaptation of an existing mechanism, rather than the establishment of an entirely new system. However, a global system or registration for cross border transactions would provide for greater co-operation among countries and may result in higher levels of compliance by users.

6. In order for the registration model to be feasible, specifically for business-to-consumer transactions, it would be necessary for suppliers to be able to determine the consumption tax status of their customers. This is a major issue. In addition, the identification of foreign businesses that supply on-line services or intangible property to customers is also a major issue.

Customer status

7. The supplier must be able to determine the consumption tax status of his/her customer to apply the registration model. An EU-supplier can check the authenticity of the VAT identification number of the customer with the tax authorities in the jurisdiction of the customer. If the VAT identification number is not authenticated then the customer can be treated as a consumer. When dealing with cross border transactions, the following questions arise. Is it technically feasible to implement such a control feature on a global scale? Could VAT authentication information be included or integrated into digital certificates that are being currently developed for use in e-commerce. Are there any other technical (or other) alternatives available for determination of the consumption tax status of the customer?

Jurisdiction of the customer

8. A number of options have been identified which might be useful in verifying the jurisdiction declared by the customer. Such options include, IP numbers, digital certificates and credit card information. These options are discussed in depth in Annex VIII, IX and X. Further evaluation of each of these options would be required to determine an order of priority from a feasibility, effectiveness and cost point of view.

Non-resident supplier identification

9. Technically, the identification of non-resident businesses that supply on-line services or intangible property to customers will be a major issue. The question here is can technology identify and authenticate the non-resident supplier of on-line services and intangible goods? Four primary options are worthy of consideration from a technology perspective.

10. First, can the payment system provider supply such information. In general, before a merchant can process a credit card payment, it needs to submit an application to the payment system provider and have the application approved. As part of the application process, the merchant must declare that transaction will be on the Internet, since Internet transactions are classified by credit card associations as a "Card Not Present" transaction (the same classification as a mail order/telephone order transaction).[1] Therefore, the payment system providers are capturing information on suppliers who had transactions on the Internet. However, payment system providers do not normally have descriptions of sales, so that it will usually not be possible for those providers to identify suppliers who had transactions of in-tangible goods and on-line services on the Internet. Annex V provides more information on how credit card sales are facilitated. The conclusion however appears to be that the payment system provider will not be able to assist in identifying non-resident businesses making suppliers into a jurisdiction.

11. In addition, the threat from electronic cash appears to have subsided. In general, electronic-cash transactions are treated similar to cash transactions, therefore, information available from payment system providers would be limited to amount of transaction. However, despite the hype of electronic-cash few years ago, market acceptance has been low. Therefore, electronic-cash shall not be major concern in the short term. It will be worth watching developments in this area, with Mondex currently gaining a degree of market acceptance.

12. Secondly, the use of search engines (including meta search engine, a program which issues a query to several Internet search engines at once) to locate the web sites of non-resident suppliers may not be useful. Many web sites only provide little information about its physical business. This fact is already an issue identified by revenue authorities, consumer organisations and others concerned with identification on the Internet. In addition, many nations permit the registration of a domain name under their country code even if the site is owned, operated and maintained elsewhere.

13. Third, certification authority or registration authorities have been considered. Certification Authorities (CA), which issue digital certificates, should be able to provide information on web site owners as long as the CA's registration process are properly operated. In addition, if a CA is also a payment system provider, the CA will be able to identify non-registered supplier who conducted business with local customers. However, since payment system providers do not necessary have descriptions of sale, it will be

1. The level of identification of Internet facilitated transactions is likely to increase with credit card companies having recently expanded their data set to include a specific code to be used on Internet facilitated transactions.

difficult for those providers to identify which supplier had sales of intangible goods and on-line services. Further investigation is required in this area. The feasibility of this option would be strongly dependent on the role TTPs would play in the settlement of Internet transactions. In this regard, the use of digital signatures and their underlying certification procedures continue to evolve; it seems likely that authentication by TTPs will be a central element in e-commerce.

14. Fourth, exchange of information may have a role to play which would include the use of spontaneous exchanges of information between the tax authorities of the jurisdictions of supply and consumption. As suppliers have to make a tax declaration for consumption tax purposes in their own jurisdiction, tax authorities may become aware of the international transactions of domestic suppliers when auditing the suppliers' accounts and records. This information could be passed on to the tax authorities of the jurisdiction in which consumption takes place. The technology issues here are limited to the implementation of secure data communications and data/transaction standards between administrations. The main difficulties will be in implementation *i.e.* international treaties, compliance etc. However, given the relatively small percentage of businesses subject to field activity in a year, this option suffers from a lack of robustness.

Compliance burden on the non-resident supplier

15. An important drawback of the registration system is that it would impose significant compliance costs on non-resident suppliers, particularly those making supplies in multiple jurisdictions, and those making supplies of nominal value. The WP9 Sub-group Paper recommends the development of a range of electronic services in order to ease this compliance burden. Such facilitation could be achieved through the provision of easily accessible information on the Web or an enhanced system to provide a goods classification and calculation routine on the Web.[2] This solution is an important component of each of the following collection model options.

2. See the discussion on online registration and filing in Annex XI.

ANNEX IX:
TAX AT SOURCE AND TRANSFER

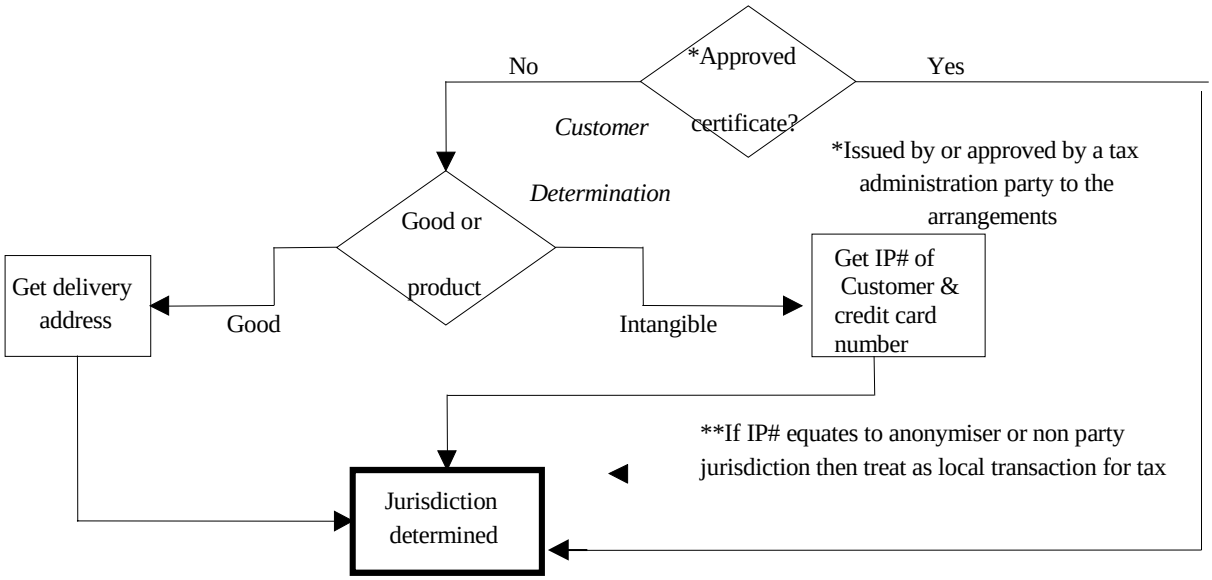
1. A detailed model of how a tax at source and transfer option works is at the end of this Annex. The important features of this option can be summarised as follows:

Nature of purchaser

2. Indirect taxes only apply to consumer sales, therefore if the purchaser provides proof (a business registration number or digital certificate for example) of being a business, no tax is imposed.

Determine jurisdiction

3. The following diagram illustrates this part of the model and has been extracted from the full model.



4. Several technologies/methods may be used to determine the consumer's jurisdiction.

5. If the consumer offers a digital certificate approved by their local taxation administration, the jurisdiction will be specified and the transaction can proceed on this basis. (Note that this provides an incentive for taxation administrations to work with digital certificate providers, further increasing their acceptance and use in all Internet transactions.)

6. While robust digital certificates, specifying jurisdiction in attribute fields, offer the greatest reliability in determining jurisdiction, their widespread acceptance and use by consumers is still in the order of three to five years away. In the absence of a digital certificate, other tests will need to be invoked as follows.

7. Parties would normally be required to disclose their addresses for entering into an on-line transaction. Addresses disclosed by parties, however, may not be fully relied on for fiscal purposes by all governments and further proof may be required by some jurisdictions. This problem is less acute in the case of purchases of goods, in these instances, the jurisdiction can be determined from the delivery address.

8. For services and other intangibles (such as electronically delivered products) the jurisdiction can be primarily based on the consumer's address as disclosed to the vendor. This can then be verified through independent checking mechanisms. This includes the consumer's Internet Protocol (IP) number (which can be obtained using software as discussed below) and other authentication methods as discussed in Annexes IV, XII and XVI.[1]

Determine tax payable and remit to local tax authority[2]

9. Most jurisdictions apply different rates to specific groups of products. In order to apply the appropriate tax rate, it will be necessary to classify the product. The United Nations Central Products Classification System is an example of a system, which may be used to cross reference classifications.[3]

10. Now we know the jurisdiction and the product, a database lookup can provide the appropriate tax rate to apply to the value of the sale[4]. This database could be maintained by a central authority and made publicly available on a website so businesses would always have access to the correct information. This feature is already available in several commercially available packages. A fee based on usage could cover the maintenance costs of the database. Alternatively, revenue authorities have an incentive to ensure their own data is always correct and current.

---

1. A similar approach to using a range of information to identify geographic information has been used by NetGeo. Using all available geographic information about a network entity, NetGeo determines the most probable latitude and longitude and gives a gauge of the reliability of the result. See "Where in the World is netgeo.caida.org?" available from: www.caida.org/outreach/resources/pspers/inet_netgeo/.

2. Some commentators have suggested that the indirect tax system is too complex to be modeled even with current computer and Internet capacity. This is easily disproved as these aspects of this model are already available in existing commercial products which offer sales / use tax calculations for the approximately 6 400 jurisdictions in the US. For example Taxware International Inc's SALES/USE Tax System "completes the tax calculations while taking into consideration all tax jurisdictional issues, exemption processing, product processing, special or standard rates based on taxing location of city, state, ZIP code and county, as well as any maximum rates." (See www.taxware.com/Zproducts/salesuse/sutaxsys.htm). Taxware's products are already incorporated in a number of third party e-commerce systems including IBM's *Net.Commerce*. The jurisdictional verification features of the tax at source and transfer model constitute the main difference to the products already offered by Taxware. The model offered by TraceWare (www.digisle.com) combines jurisdictional verification features to commercially offer a product very close to the tax at source and transfer model.

3. See www.un.org/depts/unsd/class/cpcprof.htm. It should also be noted that the CPC is currently under revision and is not globally accepted.

4. See Annex XI for an evaluation of the calculation and invoicing technologies.

11. Once the seller has calculated and retained the tax payable on the transaction, the tax can be remitted to its local tax authority in the normal manner and accompanied by jurisdictional information[5]. The local tax authority can then remit amounts to other jurisdictions on a periodic basis after deduction of an appropriate small percentage to cover their collection costs.

Effectiveness

12. From a business perspective the tax at source and transfer model is effective in that the business is only required to deal with its local revenue authority. This will minimise business' compliance costs.

13. Using technological solutions in the determination of which jurisdiction has taxing rights may provide effective coverage of taxpayers liable for tax on remote cross border sales. For example, TraceWare claims 96% accuracy in determining jurisdiction.[6] These claims have not been verified by external sources as TraceWare's techniques are patent pending and proprietary and may be subject to substantial exceptions where anonymising technologies, Internet aggregators (*e.g.* large corporates, AOL) or proxy servers are used.

Effect on consumers

14. A tax at source and transfer collection model achieves neutrality and equality of taxation treatment between traditional and electronic sales. Therefore consumers purchasing decisions are not influenced by differing tax treatments as is the current case with cross border sales in the United States[7].

Compliance burden to vendors

15. Tax at source and transfer poses some additional burdens on the vendors entering into remote cross border transactions. However, technology may provide efficient solutions reducing these burdens to relatively insignificant levels. Taxpayers also benefit from only having to deal with their local revenue authority and comply with their local laws, audits, etc.

---

5. See Annex IV for an evaluation of the reporting and tax remittance technologies.

6. *Traceroute* enquiries are readily available through many sites on the Internet. Annex II presents a visual *traceroute* enquiry on the United States Advisory Commission on Electronic Commerce homepage using Visual Route which also presents a visual map of the route between our ISP in Canberra and the ACEC in Richmond, VA. This program is available for purchase from www.visualroute.com.

   Another such example is TraceWare, which claims a 96% accuracy rate of determining the location of the customer. Further information on TraceWare can be obtained from www.digisle.net .

7. For example, Goolsbee has suggested that this is a motivation for 25 - 30% of online spending (Goolsbee, Austan, "In a world without borders: the impact of taxes on Internet commerce", November 1998, page 5, available from the American Commission on Electronic Commerce's website at www.e-commercecommission.org).

Administrative burden

16. The WPP Sub-group Paper proposes that additional costs incurred by local tax administrations may be recovered in the form of a retained percentage of foreign tax collections. Therefore the impost to tax administrations will be minimised causing no primary concerns.

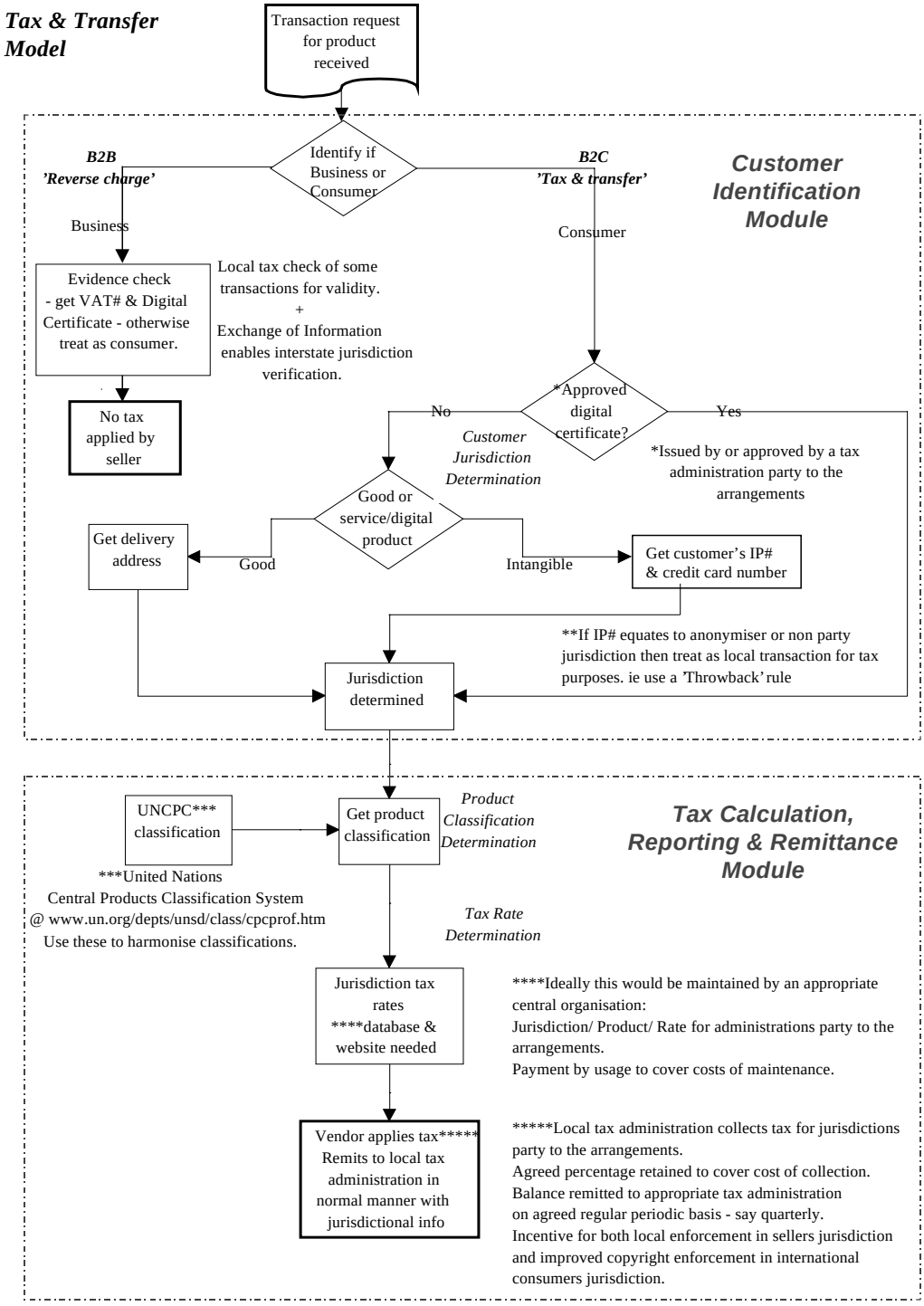
Changes required to facilitate implementation

17. Technology currently exists to enable a successful implementation of the tax at source and transfer model. The model is also flexible enough to benefit from future improvements in technology and the adoption of new technologies by business and consumers.

18. The model will require agreement amongst governments for implementation. These agreements will need to facilitate the collection of other countries' consumption taxes from businesses by the revenue authority in their jurisdiction. A mechanism for transferring revenues between countries will also need to be agreed.

19. Bilateral agreements may prove to be the most practical and feasible option to advance implementation of the model. An alternative may involve the use of the existing OECD / Council of Europe (CoE) Multilateral Convention on Mutual Assistance in Tax Matters as a basis for furthering these collection arrangements.

Detailed tax at source and transfer collection model



ANNEX X:
TRUSTED THIRD PARTY MODEL

1. A detailed model of how a trusted third party option works is at the end of this Annex.

2. The TTP model is in large part identical to the tax at source and transfer model. The difference is that a trusted third party is charged with responsibility of collecting the tax rather than the local revenue authority. This changes the last step in the diagram of the two models. A related difference is that a private third party would only undertake such a role with a profit incentive while a revenue authority will be more concerned with merely covering their costs of collection given their broader role in society. Some governments, such as the *US* have decided that tax collection systems are best and most efficiently handled by the private sector, and thus it is not "a given" that government can perform the tax collection role more cheaply than the private sector even if the latter has a profit motive.

3. The issue of who pays for the cost of collection is a critical one. The cost of compliance may be diminished by a number of factors such as:

1) The availability of suitable global technological solutions and standards on a large scale
2) The creation of a process which limits and preferably eliminates errors in advance
3) The assignment of tasks to the party in the overall system who is the most "competent" or "able" to provide it – a government would know its tax rules better than a remote vendor.
4) Simplification of the tax systems
5) Harmonisation of tax systems

4. Another factor relating to the cost of collection is the issue of who benefits from the time value of holding the funds for the period from when the money is collected from the consumer to when it is remitted to governments. Currently, the supplier who holds the liability for tax collection, enjoys the benefits of this positive cashflow. Under a TTP system, the TTP could share in the benefit received by suppliers depending on their relative contributions to the process, or could remit funds to the government immediately. The windfall received by governments in this latter instance could be used to provide partial compensation to the TTP and to reduce the role and therefore the liability of the vendor. In addition, vendors could also pay a fee for the TTP for the service, which they are receiving as part of an end to end business system. In such a system, the tax module is generally small relative to the other business modules such as order processing, inventory management systems etc. which are being utilised by the vendor.

5. The mode of operation of the TTP can vary depending on the circumstances. It would perhaps be most efficient for the TTP to operate from regional sites, which would be linked globally. It is also possible for the TTP to operate on a country by country basis depending on the relative costs and availability of telecommunication facilities.

6. A possible means of achieving greater accuracy on the TTP model would be if the trusted third parties had access to a means of verifying the jurisdiction of the consumer. The client databases of the financial institutions (*e.g.* bank or credit card companies) that facilitated consumers' electronic transactions may contain such information. Access to the client databases would provide the necessary information to perform crosschecks between the address declared by the consumer and the credit card billing address. This would presumably provide a higher level of accuracy than available in the tax at source and transfer mode however it would require not only acceptance by all major financial institutions to be viable, but would need to conform to

privacy rules and considerations. This agreement and acceptance by financial institutions is likely to be difficult to achieve.

Effectiveness

7. This option may provide an effective mechanism for the collection of taxes on remote cross border sales, but would require "team work" and an overall systems approach among vendors, TTP and governments who are parties to the tax transaction.

Effect on consumers

8. None, this process would be transparent to consumers and would not appear to be any different than the system in place today, where the vendor collects the tax. In fact, the consumer would have greater confidence that the tax paid over to a TTP (subject to government audits) would indeed be remitted to the government of his jurisdiction than he would have if remittances of tax were paid over to remote/foreign vendors over whom his government would have no direct enforcement authority.

Compliance burden to (vendor)

9. The trusted third party option reduces the burdens and liabilities of the vendor by taking over the tasks of calculating, billing, collecting, reporting and remitting to government. In addition such an integrated approach, if available for more than just "virtual products" could provide to the business community with an opportunity to participate in the global marketplace with relative ease, reduced cost and increased speed to market.

Administrative burden

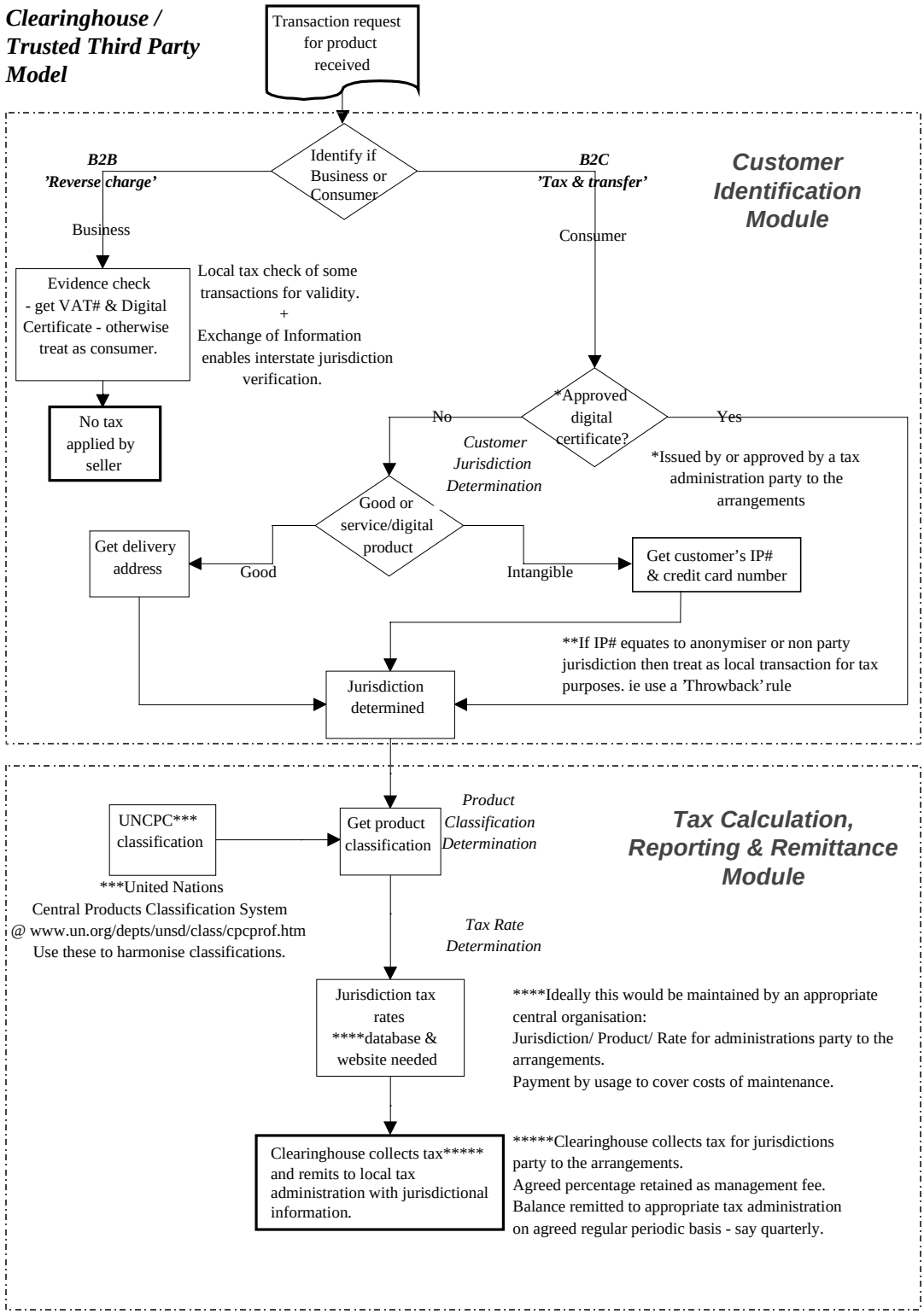
10. Additional costs would be incurred by tax administrations in establishing a new system. Governments would be required to do some "up front" and "on going" work to review/verify TTP systems and provide certification. However, such initial investments would yield numerous benefits downstream in terms of greater accuracy in the compliance process. In addition, their duties with respect to auditing vendors would diminish. Rather than auditing each vendor in their jurisdiction for all parts of the compliance process, they would audit only their approach to classification of goods and connectivity. In addition, they could perform systems audits of a limited number of TTPs, which would undoubtedly provide governments with more "coverage" and be more efficient and less costly on an overall basis.

Changes required to facilitate implementation

11. A number of issues need to be addressed and agreed upon at an international level before such a model could be adopted. One of the most pressing issues which needs to be addressed before such a model could be implemented is the legal duties and obligations of each party in the process. This includes: vendors to classify and connect, TTPs to perform the collection process and governments to audit their local vendors and provide tax verification services to the TTP.

12. Finally, there is the challenge of selecting the TTPs. As we have seen from above there may be additional costs to bear and one such way to minimise the additional costs is through competitive markets. This in itself may cause a number of difficulties within the market as some TTPs would be more efficient than others, resulting in the potential for market distortions. It is anticipated that large providers or world class consolidators of e-commerce facilities will emerge once the tax collection process is settled.

Trusted Third Party - Models



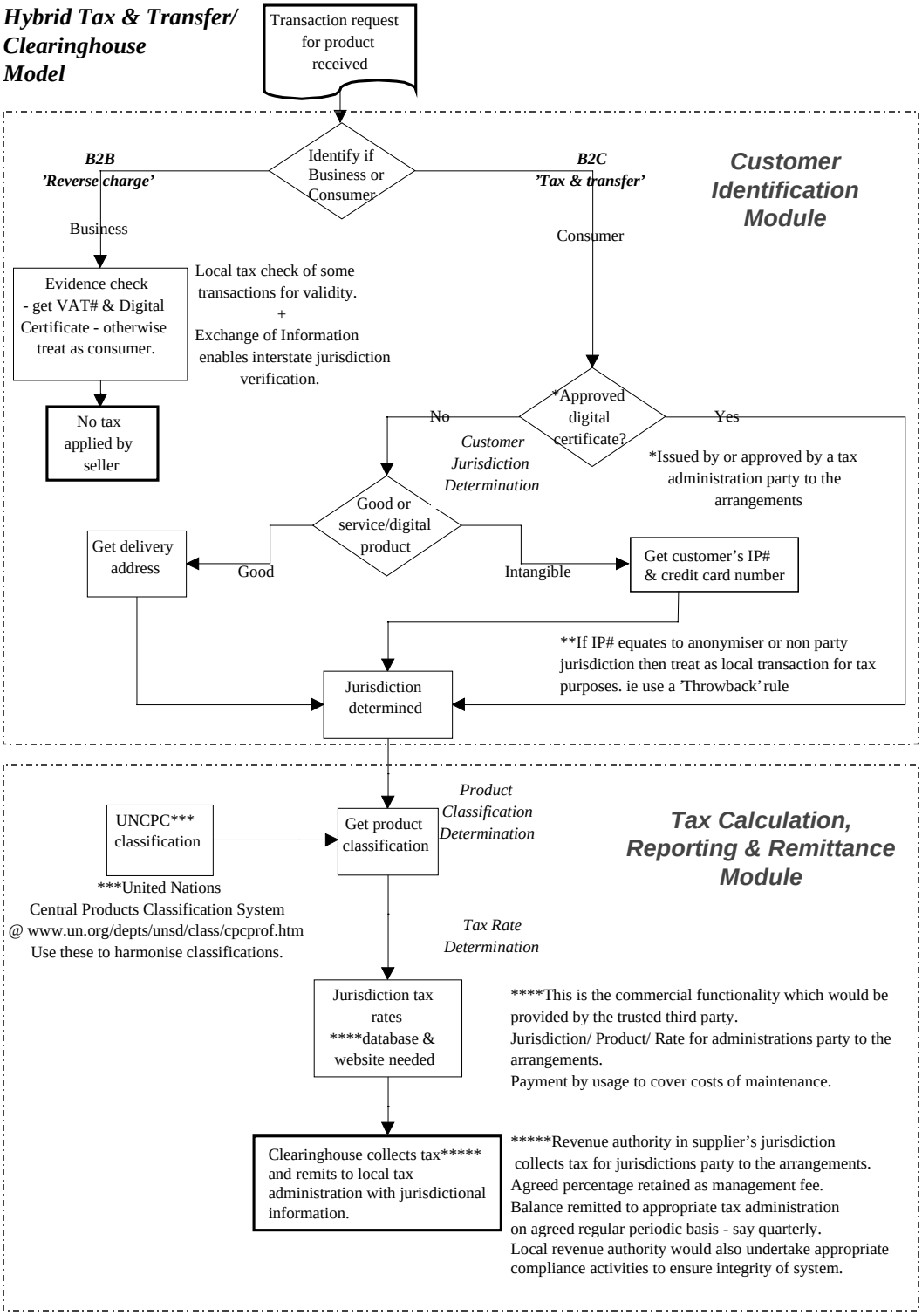
ANNEX XI:
HYBRID TAX AND TRANSFER/CLEARINGHOUSE MODEL

1. The strengths and weaknesses of these two models in some ways counteract each other. An alternate approach may be a hybrid one that takes parts of both the tax at source and transfer and the clearinghouse models. A model is shown below.

2. This hybrid model would operate by having a trusted third party provide jurisdictional identification, tax rates, product identification and tax calculation services to businesses selling products electronically. This would be similar to those services already offered by TaxWare and TrustWare and IBM Global Merchant as discussed above. Their fees would be collected from businesses using the service, a collection fee paid from the revenue authorities or both.

3. However rather than having these trusted third parties extending their operations into the collection of revenue and the associated compliance activities, some governments may decide to assume those functions themselves. These governments may view this activity as a minor extension of their current role allowing them to use their existing compliance powers and systems to ensure the successful operation of the system. This is presumably drawing on an area in which they have legal authority, a competitive advantage and existing expertise. In any event, whether a TTP or a government performs the collection activity, revenue authorities would have the responsibility of providing up to date and accurate information on their taxation rules to the trusted third parties.

Hybrid tax and transfer/clearinghouse model



ANNEX XII: IDENTIFICATION OF BUYERS, SELLERS AND JURISDICTION

		IP address	Digital certificates
Technology	Use of the technology	Use IP addresses as an indication of jurisdiction	Use a digital certificate (issued by relevant authority) that is used for each transaction and contains jurisdictional information in attribute field
Effectiveness	Accomplishes intended goal	Some well known situations in which it doesn't work (e.g. AOL for N America and Canada, and anonymisers), but suitable for majority of users	Yes
	Minimises fraud	Yes, for majority of population when used in a two out of three type situation to indicate jurisdiction	Yes
	Protects Privacy	Yes (no extra information over existing usage)	No
Feasibility	Availability	Yes. Utilities such as traceroute are readily available, as are commercial variants such as VisualRoute. TraceWare from Digital Island claim high effectiveness through a combination of IP addresses and other technologies that they have	Not widely available at present
	Ease of deployment	Easy (relative)	Difficult (needs full PKI)
	Desirability of Government pilot project to develop a solution		
	Cost of implementation	Low (relative)	High (relative)
Impact	Burden on the Internet performance	Low (main impact is on merchant server and database used for lookup)	Uncertain, needs PKI infrastructure to exist current implementations may slow transactions and add complexity
	Consumers	Low	High
	SMEs	Low (need upgraded merchant software)	
	Large Business		
	Tax Authorities	Low	High (need to participate in PKI)
Global acceptance indicators	Issues promoting global acceptance	Data available to set up mappings	
	Issues hindering global acceptance	Move to IP6 has unclear impact	Needs PKI
Changes required to facilitate implementations		Merchant software used by retailers needs to be updated. Online database of data to be built	Global PKI needed.

ANNEX XIII:
FILING AND ELECTRONIC PAYMENTS

Introduction

1. The WP9 Sub-group Paper recommends the development of a range of electronic services in order to ease the taxpayer compliance burden. This is seen as particularly important in the Registration collection model where the registration system would impose significant compliance costs on non-residents, particularly those making supplies in multiple jurisdictions, and those making supplies of nominal values.

2. The following services were identified as important in this context:

Development of an on-line tax return filing system.

Development of an on-line tax registration system.

Development of an on-line tax payment system.

Provide sufficient easily accessible information on the Web or an enhanced system to provide a goods classification and calculation routine on the Web.

3. This paper addresses the technical issues with regards to the development and implementation of an on-line tax return filing system and on-line tax registration system.

Internet - registering for consumption tax and filing tax returns

4. The Internet provides a cheap and widely available communications system for information exchange. This system can be harnessed by revenue authorities and used as an alternative to land post for the delivery and receipt of Tax returns and Registering for VAT/sales/consumption tax with a revenue authority. In addition, the Internet facilitates many other taxpayer value added support services, the delivery of which would be less practical using land post.

5. These services include:

Taxpayer access to their own tax information held on Revenue files.

Information and calculation support for the assessment of tax liability.

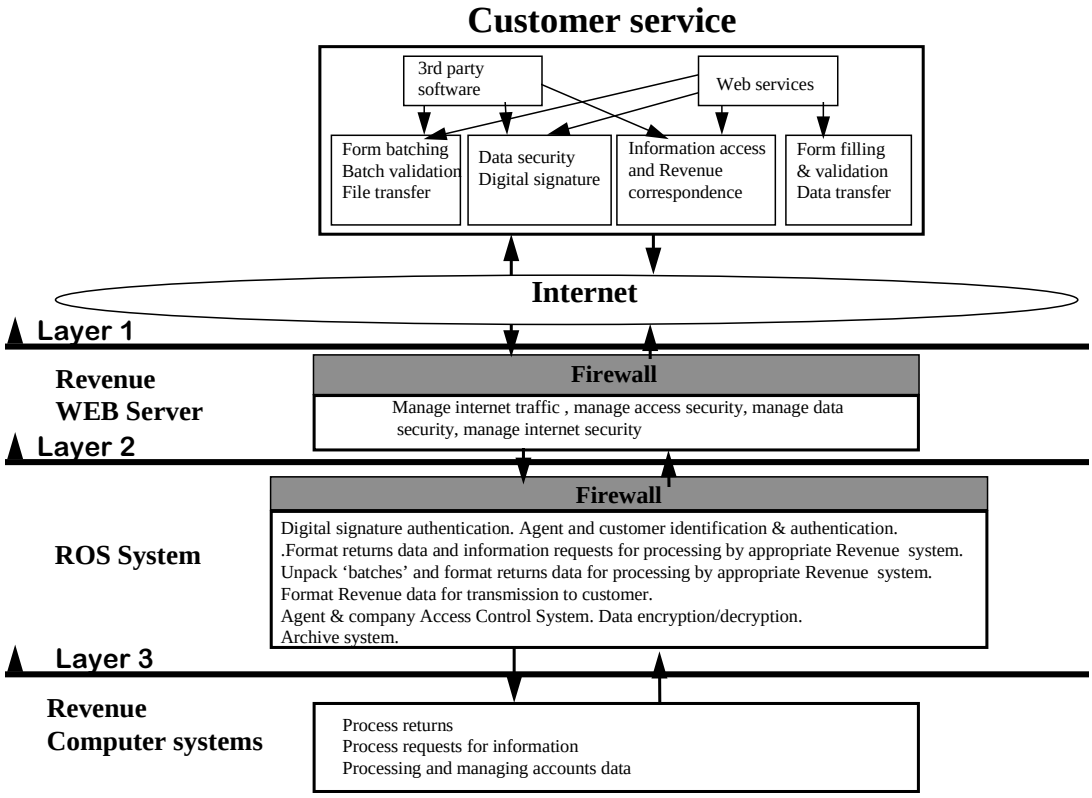
Rapid interactive communication.

6. Currently many revenue authorities are giving serious consideration to this alternative communications system for the filing of returns. Australia (Income Tax & VAT), United Kingdom (VAT), New Zealand (employer withholding tax), Spain (VAT), US Internal Revenue Service and a number of US states among others have introduced tax return filing over the Internet. France and Ireland are currently

developing systems for filing tax returns over the Internet. The Irish system will be released for use in September 2000.

Functional outline description of an Internet system

7. This figure provides a high level description of the functions of the Irish Revenue's Revenue On-Line Service (ROS). (A high level process flow diagram is also included at Annex XVIII.)



8. Most of the functions described above are standard and would apply to any tax return filing and registration system. The methods used for delivery of each function may differ e.g. a different method to Public Key Infrastructure (PKI) Digital Signature may be favoured by some revenue authority for the provision of taxpayer identification, authentication, checks on the integrity of data submitted and non-repudiation of the transaction by the sender.

9. The functions of an Internet system would include (among others)

A customer interface which is easy to use, informative, reliable, attractive and stable.

Access to the Internet site of the required revenue jurisdiction (see Figure 1 Annex XVII).

An option to select the required consumption/VAT or tax return form for the required return period (see Figure 2 Annex XVII).

An option to select the required tax registration form.

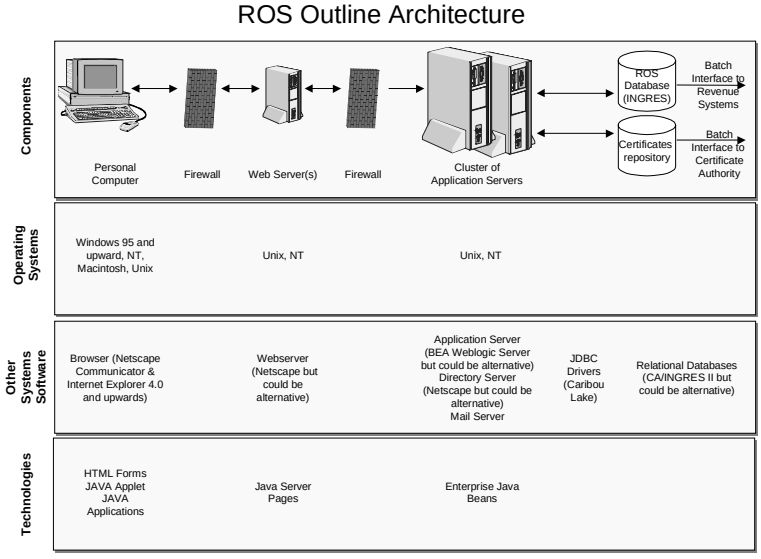
Function to complete and validate the form (see Figure 3 Annex XVII).

Function to sign and submit the form to the revenue jurisdiction (see Figure 4 Annex XVII, and see also 5.2 below).

10. An Internet based return filing and tax registration system can be provided which will work with most common computers, using most common operating systems and widely available free Internet browsers. A filing system need not be a heavy user of graphics so that it will function perfectly well with cheap readily available communications modems connected to standard telephone connections.

Technical outline description of an Internet system

11. This figure provides a high level description of the components of the Irish Revenue's Revenue On-Line Service (ROS)



12. The filing and registration system can be built using commonly available Internet programming languages, tools and hardware components. Many of the components in the above figure are interchangeable with other commonly available proprietary products.

13. The programming skills required are already widely available internationally and indeed are becoming common place. There is essentially little difference between the building of a revenue tax filing system and the build of a commercial Internet trading site such as Amazon.com. The number of quality and secure commercial trading sites is increasing rapidly and the development and maintenance costs are reducing.

Effectiveness of solution

How well does the solution fit the requirement?

14. The Internet solution fits the requirement very well.

15. The technology is readily available and widely used internationally.

16. Depending on the Identification and Authentication method chosen this solution will work perfectly well on WAP enabled mobile phones and television top Internet "boxes" (Public Key Infrastructure *i.e.* digital signature, enabled WAP and TV top box devices are new to the market)

17. The functionality required is suited to the Internet.

18. Use of the Internet is growing as access gets easier and cheaper and the range of useful services increases.

How secure is this information?

19. Security issues still dominate the Internet debate.

20. The key essential security issues are:

1) Identification and authentication of the parties in a communication/transaction.

2) Signature of parties to a contract or legal document.

3) Guarantee of the integrity of a communication or transaction *i.e.* proof that what was sent is the same as what was received. This is necessary to prevent the sender repudiating the transmission or content of the transmission.

4) Confidentiality of data in transmission *i.e.* that no one other than the sender and receiver can read the data.

5) Protection of data stores and Internet sites from hacking. This includes denial of service attacks, data theft, access to confidential data and corruption and defacing of an Internet site.

21. At this stage the debate surrounding items 1), 2) and 3) above is polarising into supporters of Public Key Infrastructure (PKI) *i.e.* digital signatures, and those who support alternative methods. Organisations who have implementing or are implementing PKI include Identrus, Australian Tax Office, New Zealand Tax Office, Ireland Revenue, Citibank, Bank of Ireland, Bank of Scotland, Sydney Stock Exchange.

22. PKI *with supporting legislation* will support the requirements at 1), 2) and 3). The arguments appear to centre around possible easier ways to achieve the same result and on the possible impediments to the proliferation or take up of PKI as an internationally accepted standard.

23. Security item no 4) - confidentiality, has a more stable and accepted solution. Strong encryption products are now available internationally since the relaxation of US export restrictions on these products. Standard browsers can now be enabled remotely e.g. by the revenue authority, or trusted third party, providing the revenue Internet service, to support strong encryption. This level of encryption is currently accepted as being sufficiently secure to provide data confidentiality.

24. Security item no 5) - hacking and denial of service attacks. Hacking has had a high profile recently with attacks, in the main "Denial of Service"[1] attacks, being perpetrated on a number of high profile sites. In the main, a good quality and actively monitored security plan and a system configuration incorporating strategically placed and properly configured "firewall" systems, anti virus systems and tools for monitoring inappropriate site activity will reduce the possibility of successful attacks. But there is no total protection.

Are there any data protection issues with storing, disclosing and processing information?

25. Identification, authentication of the correct taxpayer and confidentiality of correspondence were the data protection issues which arose in the context of the services being provided by the Ireland revenue. The Data protection commissioner was satisfied with the use of Public Key Infrastructure with supporting legislation and an approved Certificate Policy Statement.

Feasibility of solution

Availability of solution and accessibility to the solution

26. Australia Tax Office, New Zealand Tax Office, UK Customs and Excise (VAT), Austria Dept. of Finance, Ireland Revenue, Singapore, US state of Indiana, US State of Idaho, Spanish Mint are among those authorities who have or are just about to implement Internet filing of tax returns. This list will grow rapidly over the next year or so.

27. Standard suites of "off the shelf" solutions will become available within the next few years. Because of the commonality of tax return filing functions across revenue authorities these "off the shelf" products will only require minor modification for each administration.

28. One major overhead which will impact on each administration will be the development of a system to "interface" information backwards and forwards from their own core revenue administration computer systems to the new Internet filing and registration system. This development effort should not be underestimated and, depending on the technology used in the core revenue computer systems, may exceed the cost and development time of the Internet system itself by a considerable amount.

Deployment of solution

29. An Internet filing system is easy to deploy technically. The administration hosts the system and anyone anywhere who is connected to the Internet has the potential to access the system.

30. The key issue here is the roll out of Identification and Authentication security. As yet there are no international agreements in place to give international recognition and legal standing to an internationally available digital signature provided by an internationally approved and accredited Certification Authority[2].

---

1. Denial of service attacks are caused by continuously bombarding a site with thousands of transactions until the site overloads and fails

2. Trusted third party who will manage and be legally responsible for the identification of the person receiving the digital certificate, the ongoing monitoring of the authenticity of the issued certificate and the maintaining of the security of the certificate system.

However, considerable work is being carried out at both European level and internationally for international standards and interoperability.

Expected useful life of solution

31. Internet technology is improving at a rapid rate. The functionality of a filing and registration system is not likely to change and will have a long useful life. The method of delivery or the design of the delivery system is likely to evolve with changes in technology.

Who should supply the solution

32. The service can be built and provided by the revenue authority itself or, alternatively, the service can be built, provided and hosted by a trusted third party. This latter alternative may be attractive as it could allow for many administrations to avail of the services of a single trusted third party. The benefits would include cheaper start up costs, common standards and look and feel, easier system for the taxpayer who may be filing returns to more than one jurisdiction.

33. An additional benefit is that the trusted third party would be in a position to provide value added services to international customers. These services could include a managed tax system where the third party processes the suppliers Internet sales, identifies the consumer, applies and deducts the appropriate tax and finally files and pays the appropriate tax to the appropriate jurisdiction on behalf of the supplier.

Cost

34. As referred to already at 6.1 above, standard suites of "off the shelf" solutions will become available within the next few years. Market competition should see the cost of these products reduce. However, it is currently unclear what type of pricing structure will prevail e.g. fixed initial price + annual charge based on number of users, fixed initial price + percentage annual cost or other pricing arrangement.

35. 5m Euro would be a fair indicative cost of the development of a secure Internet filing system. This price would typically include:

Development of a range of return forms (including some complex corporate tax return types).

Secure mail delivery system.

Provision of a taxpayer information system to allow a taxpayer query his or her own personal information stored on revenue files.

PKI enabled digital signature, identification and authentication, data integrity and data confidentiality.

The price is likely to exclude:

Development of core system interfaces.

The provision of a hardware (servers etc.) infrastructure in the tax administration to support the services.

36. As mentioned earlier, one major development which will impact on each administration will be the development of a system to "interface" information backwards and forwards from their own core revenue administration computer systems to the new Internet filing and registration system.

Impact of proposed solution

Consumers

37. None.

SMEs

38. Reduce compliance cost, effort and complexity.

Large businesses

39. Reduce compliance cost, effort and complexity.

Tax authorities

i) Improve compliance, improve yield, reduce return form processing costs and processing errors.

ii) The development of filing and registration services for foreign resident suppliers should be considered in the broader context of also supplying these services and a range of other services to resident taxpayers within the administration's own jurisdiction.

Impediments to easy expansion of e-commerce

40. This solution does not provide any technical impediment to the expansion of e-commerce. However, it is arguable that the taxation of e-commerce transactions has the potential to do so but that is a taxation policy issues and is being addressed by other TAGs.

Global acceptance indicators

41. The proposed solution is a relatively straightforward e-commerce type solution conforming to the general pattern of Internet development. It provides for a useful and easy to use service over the Internet and is likely to be globally accepted.

Changes required to facilitate implementation

42. Essentially the changes required to facilitate technical implementation are legal and business rather than technical. It is fair to say however that the technical development would be useless and not capable of implementation without the legal and business changes being in place.

43. High level description of the changes requirements:

Supporting legislation within jurisdictions for acceptance of electronic forms, return form signature and Identification & Authentication of the parties to the transaction

Internationally accepted standards and agreements on Identification & Authentication of the parties to the transaction

International agreements on Certification Authority interoperability

International co-operation agreements and legislation within jurisdictions to provide for cross border Audit of returns and supporting account information

International co-operation agreements and legislation within jurisdictions to provide for cross border return compliance activity and enforcement

International co-operation to avoid a proliferation of tax-free havens where suppliers can incorporate and make supplies without deduction of tax.

Administrations should introduce special rigorous systems to identify and check and approve refund/repayment claims made by foreign resident suppliers.

Conclusion

44. The provision of Internet services for the on-line filing of consumption tax returns and the on-line registration with a tax jurisdiction for the charging, collection and submission of consumption tax is technically feasible.

45. Many administrations have implemented or are about to implement electronic filing over the Internet. Many more administrations are considering the provision of this service.

46. There is no technical reason why registration for consumption tax cannot also be provided by Internet forms.

47. However, there is a significant business issue to be addressed first. There is a potential for a person to misrepresent himself in applying for a registration. This has the potential to facilitate the perpetration of fraudulent deduction of consumption taxes without providing enforceable redress by the tax administration.

48. To permit a supplier, whether resident or non-resident, register for consumption tax using the Internet, a tax administration MUST be able to satisfy itself with regards to the identification and authentication of the applicant.

49. The identification and authentication method must also provide for non repudiation of the registration transaction by the applicant.

50. The full identification, authentication and non repudiation system will also need to be supported by legislation and appropriate inter jurisdiction agreements. This will provide a framework for enforcement and redress.

51. Digital Signature technology *i.e.* Public Key Infrastructure will deliver the technology to provide this type of identification, authentication and non repudiation. However, though this technology is quite mature and stable there are no international agreements on acceptable third party certification bodies, enforcement legislation etc. in place.

52. The EU are advanced in providing a supporting structure for this technology in Europe.

53. On the international scene, Identrus[3], is dedicated to creating a worldwide network of trusted financial institutions to remove the final obstacle to business-to-business e-commerce: trust in trading partners' identities. The technology they use for providing trusted transactions is Public Key Infrastructure.

It is likely that international standards for guaranteeing trust in trading partners' identities will be in place within the next couple of years.

3. An international organisation founded by a group of prominent financial institutions - ABN AMRO, Bank of America, Barclays PLC, Chase Manhattan, Citigroup, Deutsche Bank (including its recent acquisition Bankers Trust, which was also a founder) and Hypo Vereinsbank

ANNEX XIV:
TAX CALCULATION AND INVOICING / REPORTING AND TAX REMITTANCE

		TaxWare	IBM Global Merchant
Technology	Definition of the Technology	Commercially available software to calculate taxes due on transactions.	IT real time hosted service which performs order management, credit card clearing, facilitates fulfilment, performs international tax calculation, collection and reporting for vendors in multiple currencies and jurisdictions.
Effectiveness	Accomplishes intended goal	Yes	Yes
	Minimises fraud	Relies on merchant classification and customer information received.	Relies on merchant classification and customer shipping address to indicate jurisdiction. High-powered encryption capabilities.
	Protects Privacy	N/a	Yes, processing service performed on behalf of merchant and not transmitted to others, *i.e.* governments.
Feasibility	Availability	Yes	Yes
	Ease of deployment	Built into merchant software	GM server interfaces directly with the merchant's commerce software
	Desirability of Government pilot project to develop a solution	The establishment of a global collection model would benefit from a government pilot project	The establishment of a global collection model would benefit from a government pilot project
	Cost of implementation	Low (relative)	Low (relative)
Impact	Burden on the Internet performance	Low	Low
	Consumers	Low	Low -
	SMEs	Part of merchant software	Integrated service facilitates cross-border capability for SME
	Large Business	Part of merchant software	Same
	Tax Authorities	None under current system	None under current system
Global acceptance indicators	Issues promoting global acceptance	Already widely used for physical goods	Used for both physical and virtual goods
	Issues hindering global acceptance	Uncertain tax environment	Uncertain tax environment
Changes required to facilitate implementation		Harmonisation of tax product codes across countries for all goods would assist merchants.	Harmonisation of tax product codes across countries for all products and harmonisation of invoice and reporting requirements would assist merchants. Assumption by governments of responsibility for correctness of own country tax rules included in tax calculation modules would lead to greater accuracy.

As a further indication of the directions of electronic commerce, an Internet-Draft has recently been released showing how the ideas contained within the Internet Open Trading Protocol (IOTP) could be used in a future digital certificate manner or in the existing pervasive credit card / SSL model.[1] It also indicates that IOTP will most likely be implemented using XML.

1. The January 2000 Internet Draft "Requirements for XML Messaging, Version 1, Release 00" is available at www.ietf.org/internet-drafts/draft-ietf-trade-smlmsg-requirements-00.txt.

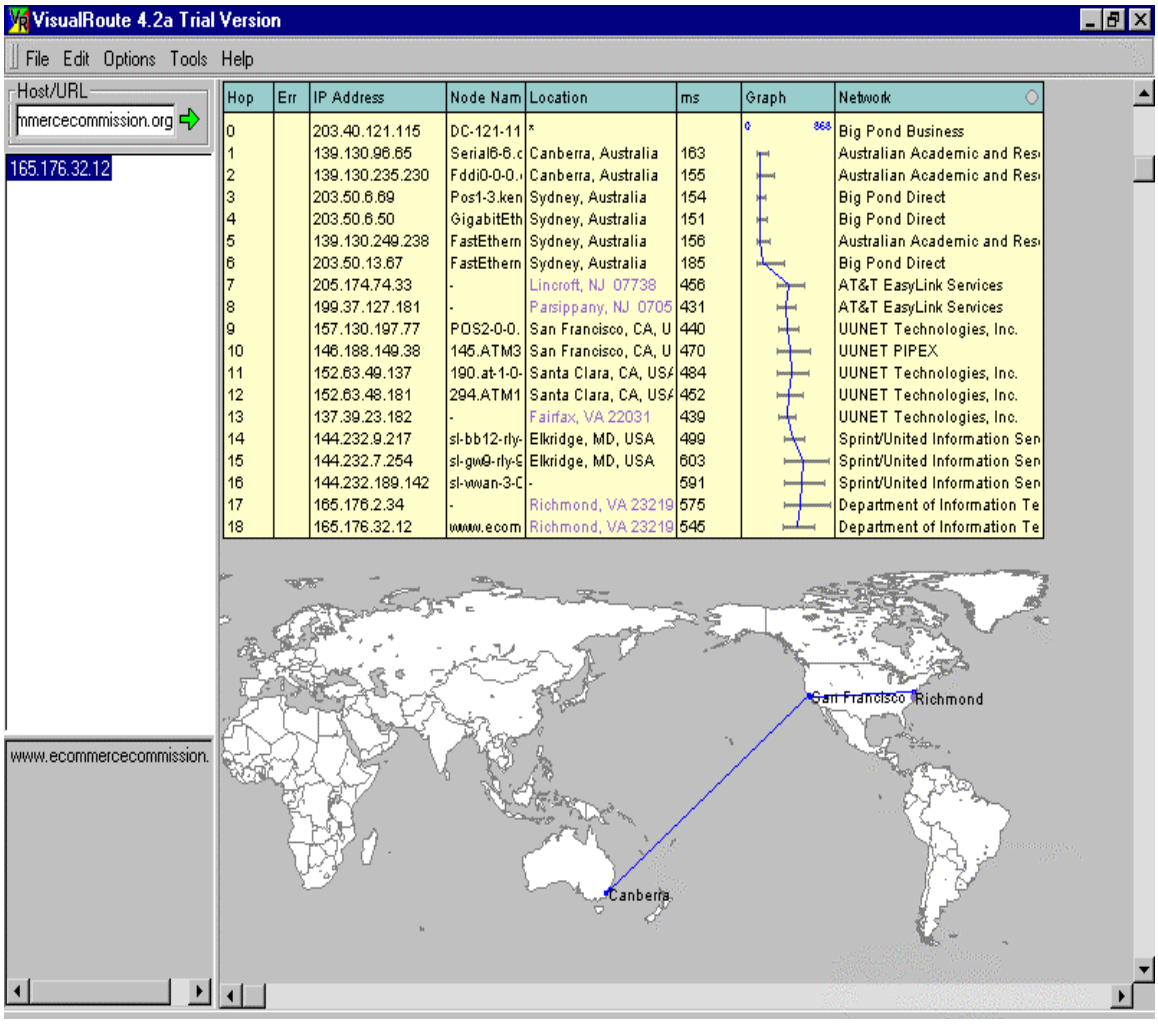
ANNEX XV:
AUDIT TRAILS

		Databases	Digital signatures
Technology	Definition of the Technology	Robust storage medium for data	Part of PKI system that provides integrity and auditability
Effectiveness	Accomplishes intended goal	Widely used to store transactional information	Very difficult to forge/tamper
	Minimises fraud	Most major suppliers contain automatic timestamping of logs etc. to prevent tampering	If certificates are issued by a respected CA and RA, then very effective
	Protects Privacy		No
Feasibility	Availability	Databases are part of most merchant software packages available today	Not widely available
	Ease of deployment	Easily deployed	Difficult
	Desirability of Government pilot project to develop a solution		
	Cost of implementation	Low to implement, but some licenses can be expensive for the retailers	High
Impact	Burden on the Internet performance	Low	
	Consumers	Low	
	SMEs		
	Large Business		
	Tax Authorities		
Global acceptance indicators	Issues promoting global acceptance	Widely used already	
	Issues hindering global acceptance	Third party access to the data.	Need full PKI to be set up
Changes required to facilitate implementations			

ANNEX XVI:
VISUALROUTE TRACEROUTE ENQUIRY[1]

1. This enquiry shows the route taken by an Internet "packet" from the ISP we were using in Canberra, Australia to the ACEC's website. We can see both visually and from the table below that their website is located in Richmond, Virginia.

2. If we were entering into a business-to-consumer transaction with the ACEC which gave rise to a sales tax liability in Richmond, this enquiry would generally have provided us with sufficient jurisdiction information to progress with the sales tax calculation through the rest of our model.



1. *VisualRoute* is available for trial and purchase from www.visualroute.com.

ANNEX XVII:
DATABASE SOLUTIONS

1. There is no insurmountable technological barrier to a Database (DB) solution for tax calculation problems. There are three main factors to address:

1) The method of calculation.
2) The categories of classification.
3) The need to and responsibility for updating the information.

Classification and calculation

2. Relational databases work off reference tables. The more tables that must be cross referenced the greater the complexity of the system. There is no need to impose the same tax amount on all products as long as the products are classified in the same manner and the types of taxes are calculated in a consistent manner. In this way, tables could identify products to classifications, classifications to tax categories and all the factors to geography and where tax must be remitted. Neither tax payers nor SMEs are experienced in the evaluation of what tax applies or how it should be calculated. Maintenance of these tables will allow industry to develop open source solutions that will provide the ability for end users or SMEs to address these issues.

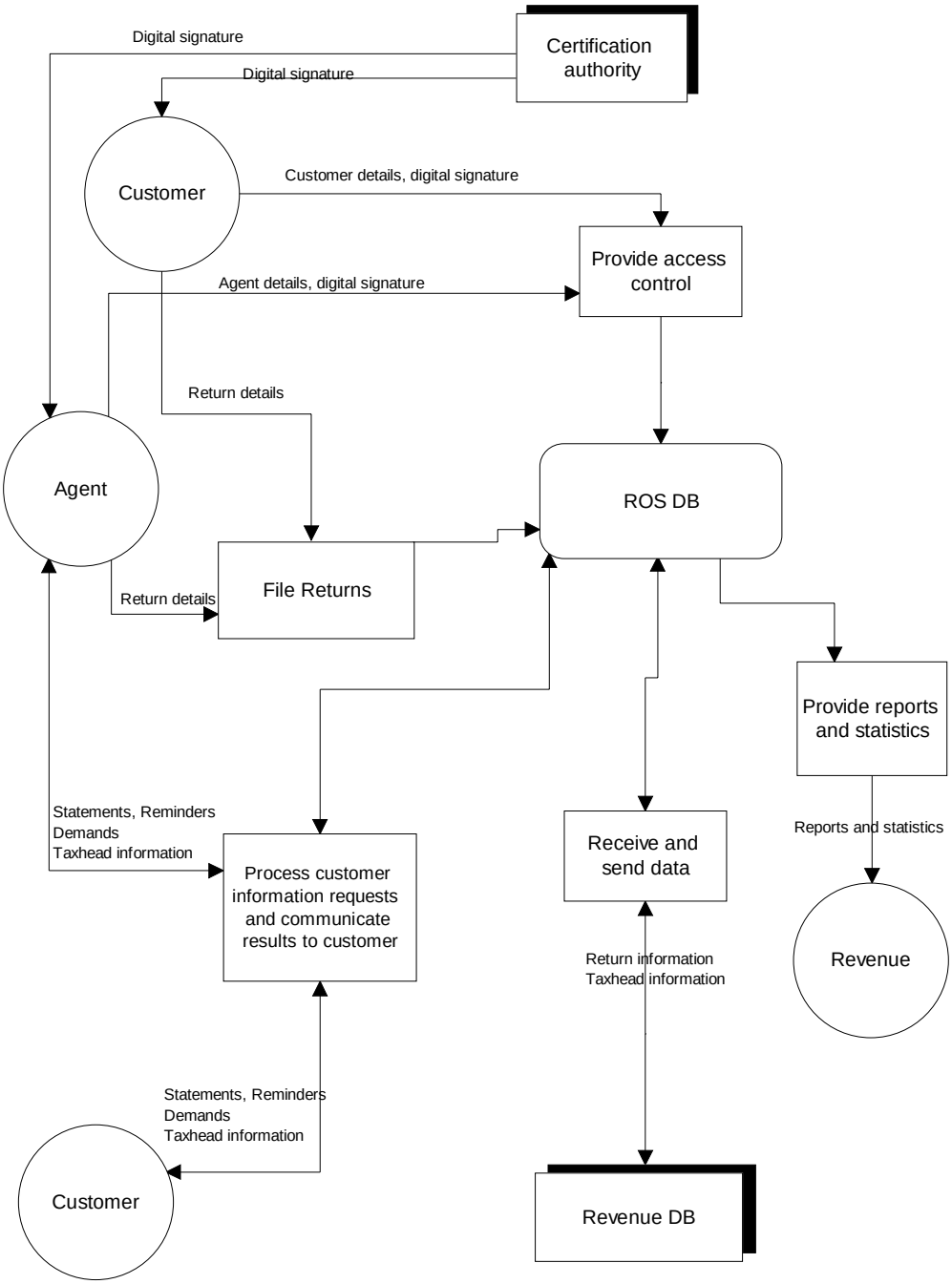
Update

3. The major issue involved in this system is the creation and maintenance of the tables. Clearly the ability to harmonise systems and methods as well as the ability to change tax amounts are factors solely within the competence of the governments of the world. It would thus be the primary responsibility of the government to maintain such tables. A set of these global tables would facilitate all four of the contemplated systems. This type of joint maintenance of tables is the only global solution for a global medium.

4. In developing any business solution, business is keenly aware of the need to provide accurate information as to complete purchase price to the consumer at the time of purchase. This not only makes good business sense but tracks the requirements of many local consumer protection laws/best practices as well as the OECD Consumer Protection Guidelines. The most likely solution would still rely on a consumer declaration of jurisdiction with minimal cross references of the consumer location via delivery address or email IP domain.

ANNEX XVIII:
PROCESS FLOW DIAGRAM

A high-level process flow diagram for the Irish Revenue's Revenue On-Line Service (ROS).



ANNEX XIX:
ELECTRONIC RECORD INTEGRITY[1]

Purpose and scope

1. In an environment such as the Internet, where records are likely to be generated and maintained electronically, questions can easily arise about the integrity of information.

2. This paper will identify and analyse possible technological solutions in preserving the integrity of electronic documents in such an environment.

3. It should be noted that the integrity of electronic documents in general, is not questioned where there are robust IT security measures and robust information management systems and procedures in place.[2]

4. Furthermore, the integrity of electronic documents is enhanced where adequate separation of duties occurs and the business adopts strong accounting and audit practices[3]

Introduction

5. The rapid development of electronic commerce has brought on a new era of transformation of global communication and trade. Electronic Commerce will potentially change the way that commercial transactions, government business, service delivery and other business initiatives are conducted.

6. For business to be conducted in an orderly, efficient and accountable manner it relies on records as reliable evidence of actions and a source of information about their activities for their own governance. On the other hand, revenue authorities rely on records as evidence of the occurrence and nature of various transactions in order to properly administer their tax systems.

7. The use of computers as part of this process, both as an adjunct to a traditional business or as a stand alone Internet business, has been enhanced by the rapid technological advances in information technology. Computers already play an important and increasingly more important role in all facets of business operation even without an Internet focus. Computers have cemented their place in the infrastructure of all businesses through:

- Falling costs per megabyte.
- Unrivalled storage capacity; and

---

1. Record integrity for the purposes of this document is taken to mean: "*The integrity of a record refers to its being complete and unaltered.*" The definition has been taken from the "*Draft International Standard: Records Management*" Committee Draft 15489-1 released by the International Standards Organisation for comment November 10, 1999.

2. For further details consult the International Standards Organisation at www.iso.org or in the United States *Model Guidelines for Electronic Records* available at www.archives.lib.de.us/recman/g-line.htm

3. For further details refer to local accounting bodies.

– Faster access speeds.

8. Whether businesses seek to convert their document storage to computer systems or operate business functions through computer interaction, they must nonetheless be careful to ensure that their systems produce and maintain records that are:

– Accurate.
– Reliable.
– Trustworthy; and
– Meet their legal and corporate obligations[4]

9. The accuracy and integrity of electronic records are not only important to the success of any business, but also take on special significance when those records are relevant to possible litigation or must be submitted to a government agency, including revenue authorities, for regulatory reasons.

10. What are the essential elements of an electronic record storage system? While there is no definitive law on the subject, there are important guidelines which may be adopted when formulating and implementing an electronic records management system.

11. The International Standards Organization (ISO) in their *Draft International Standard: Records Management* state that there five essential characteristics which should be maintained in electronic records systems. These are:

– ***Reliability:*** Record systems, procedures and practices should work reliably to ensure that records are credible and authoritative.

– ***Integrity:*** Control measures such as access monitoring, user verification, authorised destruction and security should be implemented to prevent unauthorised destruction, alteration or removal of records[5].

– ***Compliance:*** Records systems should be managed in compliance with all requirements arising from current business, the regulatory and accountability environment and community expectations in which the organisation operates.

– ***Comprehensiveness:*** Records systems should manage records resulting from the complete range of business activities for the organisation or section of the organisation in which they operate.

– ***Systematic***: Records should be created, maintained and managed systematically. Records creation and maintenance practices should be systemised through the design and operation of both records systems and business systems.

---

4. Note in IRS Rev. Proc. 97 - 22 which provides guidance to taxpayers that maintain books and records by using an electronic storage system states that the general requirements of an electronic storage system are:

   2. An electronic storage system must include:

      a. Reasonable controls to ensure the integrity, accuracy, and reliability of the electronic storage system;

      b. Reasonable controls to prevent and detect the unauthorized creation of, addition to, alteration of, deletion of, or deterioration of electronically stored books and records;…

5. The Draft Statement states that these controls may reside within a records system or be external to the specific system.

12. While electronic records offer both business and revenue authorities many advantages over their "traditional" paper counterparts, they may also contain serious deficiencies. For example, electronic records may be altered without trace or evidence of the occurrence where there are inadequate systems controls.

Establishing integrity

13. It is the data within the physical records that is required, the paper document merely being the transport for the data and the physical characteristics enable certain integrity aspects to be assumed. In a digital record system the data and the records may be used and represented independently which leads to additional problems in assuring the integrity of the records.

14. The table below contrasts physical records with digital records bringing into question the integrity of digital records:

Physical records	Digital records
The original is easily distinguished from that of a copy.	The original cannot be distinguished from a copy.
Alterations are difficult to make and may be easily detected.	Alterations can be made relatively easily and given the right environment, may be made without detection.
Signature is physically associated with the record's contents.	Signature is logically associated with the contents.
Signature is directly associated with the person.	Signature is indirectly associated with the person.

Possible solutions

15. Just as technology has brought the integrity of electronic documents into question it may also provide us with possible solutions. At the present time there are a number of possible solutions being promulgated. This paper will provide an overview of the following proposals:

- Message digests.
- Encryption.
- Time stamping; and
- Notarisation.

Message digests

What is a message digest

16. A message digest (also called cryptographic checksum) is the representation of text in the form of a single string of digits, created using a formula called a one-way hash function[6]. Encrypting a message digest with a private key creates a digital signature, which is an electronic means of authentication.

17. So, message digest + key encryption = digital signature

How do message digests work?[7]

18. A message digest is an explicit method (algorithm) which is applied to a block of data of any size and produces a small fixed size result. The result is typically 128 to 256 bits, depending on which message digest system is used. It has the property that it is impossible, as a practical matter, to modify the block of data in any way (including producing entirely new data) and still produce the same result.

19. So the message digest of some data is a completely secure handle for that data. No other data can be presented which will reproduce the same message digest.

20. It may seem hard to believe that message digests can work this well. It is worth observing that 128 bits is a very big number. The number of messages that can be represented (2^{128}) vastly exceeds the number of atoms in the universe. Calculations meant to search this number of possibilities have no chance of completing or even having a lucky success in human time scales.

21. There are many message digest algorithms used in cryptographic algorithms. Apart from their role in common digital signature algorithms they also play a role in many specialised algorithms that involve an exchange of information.

For example if we personify the computers we might imagine an exchange like this:

> A: "You tell me Y and then I'll tell you X."
> B: "If I tell you Y first you'll make up an X that will give you an advantage."
> A: "Look, here's the SHA digest of X. So I won't be able to make up X later."
> B: "OK here's Y, now you tell me X."
> A: "Here's X."
> B thinks: "The SHA digest of this X is the same as the digest I was given so I know that this X existed before I revealed Y."

Does message digesting overcome possible integrity problems?

22. While message digesting allows the detection of alterations being made to "original" electronic documents it does not overcome the potential problem associated with date and time, creation manipulation.

---

6. *One-way hash function* is an algorithm that turns messages or text into a fixed string of digits, usually for security or data management purposes. The "one way" means that it's nearly impossible to derive the original text from the string.

7. Sourced from *The Internet Report* by Philip McCrea and Bob Smart at page 128. The report is available at www.ato.gov.au as part of *Tax and the Internet Discussion Report*

Encryption

What is encryption?

23. Encryption is the translation of data into a secret code. The object of encryption is to control access to data in circumstances where physical access can't be controlled.

How encryption works

24. To read an encrypted file, you must have access to a secret key or password that enables you to decrypt it. Unencrypted data is called plain text ; encrypted data is referred to as cipher text. There are two main types of encryption: symmetric encryption and asymmetric encryption (also called public-key encryption) and.

Symmetric encryption

25. Symmetric encryption is a cryptographic technique that uses the same secret key for both the originator's and the recipient's transformation. Without the knowledge of the secret key, it is computationally infeasible to compute either the originator's or the recipient's transformation[8]

26. Symmetric encryption has a number of short falls which have led to the development of asymmetric encryption which provides a higher level of security.

Public key encryption (asymmetric)

27. A public key encryption is a cryptographic system that uses two keys:

- A public key known to everyone; and
- A private or secret key known only to the recipient of the message.

28. When John wants to send a secure message to Jane, he uses Jane's public key to encrypt the message. Jane then uses her private key to decrypt it.

29. An important element to the public key system is that the public and private keys are related in such a way that only the public key can be used to encrypt messages and only the corresponding private key can be used to decrypt them. Moreover, it is virtually impossible to deduce the private key if you know the public key.

30. Public-key systems, such as Pretty Good Privacy (PGP), are becoming popular for transmitting information via the Internet. They are extremely secure and relatively simple to use. The only difficulty with public-key systems is that you need to know the recipient's public key to encrypt a message for him or her.

8. Sourced from ISO SC 27 Standing Document no 6 "*Glossary of IT Security Terminology"* available from http://www.jtc1.org

Does encryption overcome possible integrity problems?

31. While encryption offers more robust security against manipulation of content it still does not fully address all the integrity issues identified.

Time stamping

What is time stamping?

32. Time stamping means that each document is, at the time of its creation, "stamped" using special procedures, so that it can be proven later that the document really was written at that time.

How time stamping works

33. Most time stamping systems involve the use of a Time Stamping Authority (TSA) for which a service fee is charged. The time stamp is a digital attestation of the TSA that the electronic document in question, has been presented to the TSA at a certain point in time.

34. Over time several different techniques for time stamping[9] have emerged, many of which incorporate "message digesting" and "encryption" techniques into the process to strengthen the process and overcome some of the shortfalls of encryption. For example [10]:

In order to time-stamp a message M, a user U first computes the ***message digest*** *X=H(M), where H is a cryptographic hash function. The message digest X has the following properties:*

- *It is a relatively* ***short fixed size bit-string****, typically 128 or 160 bits. This reduces the communication cost.*

- *It is computationally* ***infeasible****, given only the message digest,* ***to recover the original message****. This prevents the leakage of confidential information during time-stamping. Even the TSA is not supposed to know the content of M.*

- *Even if one has both the message M and the message digest X, it is* ***infeasible to find*** *another message M' with* ***identical message digest****. This prevents the user from modifying the content of M after time-stamping.*

Next, the user sends the message digest X to the TSA.

The TSA creates the ***time-stamp for X****, i.e. a signed message* $S = signed_{tsa}\{X,t,n,L_n\}$*, where t is the current time, n is the sequence number and* L_n *is the linking information. The* ***linking information*** *is formed from X, n and the previous time-stamps using the cryptographic hash function H:*

$$L_n = H(X,n,L_{n-1},L_m),$$

where m is the sequence number of a suitably chosen older time-stamp. This linking scheme guarantees the following properties:

---

9. Further information on the various time stamping techniques may be sourced from http://moomin.ee/'helger/crypto/link/timestamping/

10. Sourced from www.cyber.ee/research/projects.html.

- *The TSA **cannot manipulate** the temporal order of issued time-stamps without breaking the cryptographic hash function.*
- *The mathematical relationship between L_n and L_{n-1} ensures that the n-th time-stamp **was indeed issued** after the (n-1)-st one.*
- *The good choice of the sequence number m (depending on n) provides efficient method for between the time-stamps issued.*

*In order to **compare two time-stamps**, one has to compose a chain of intermediate time-stamps linked together mathematically via the hash function. So one obtains the **linking chain**.*

Does time stamping overcome possible integrity problems?

35. Many of the time stamping methods offered by various TSA's which combine encryption techniques within their time stamping service overcome many of the potential problems identified earlier as being associated with electronic documents. For example, where the TSA's service takes a "fingerprint"[11] of the electronic document and certifies the time and date. This may overcome such associated problems by attesting that the contents, including any identifying information of the electronic document have not been altered since they were time and date stamped. While it does not overcome the shortfall of distinguishing between the "original" and a "copy", it does however, verify that the "contents" of the document has not been altered since it was time stamped. Thus the integrity of the document remains intact.

36. See Annex XX for a paper from CertifiedTime on "proving the time of transaction occurrence".

Costs associated

37. The costs associated with the services provided by TSA's depend on a number of factors such as, volume and type of process. For example, the cost of "Fingerprinting" and time stamping ranges from a flat fee of USD $0.50 per file[12] to others who scale their fees ranging from USD $1.00 per file up to 5 000 files to USD $0.13 per file for in excess of 1.5 million files[13]. Some TSA's also charge a fee for each time you require a file validated, these range up to USD $0.05 per validation.

Notarisation

What is notarisation?

38. In traditional terms a notary is empowered by legislation to officially attest to the validity of documents and to witness live signatures. However, the functions performed by a notary are changing with technology.

---

11. *Fingerprint* is a unique number calculated from the contents of your electronic document. If the file's contents were to be changed at a future time, even by one character, a different number would be returned thus detecting the alteration.

12. See firstuse.com for details.

13. See surety.com for pricing structure.

39. According to the ISO, notarisation is the registration of data with a trusted third party that allows the later assurance of the accuracy of its characteristics such as content, origin, time and delivery[14].

How notarisation works

40. There is little differentiation between how modern notarisation occurs and that described above in the section on time stamping.

Does notarisation overcome possible integrity problems?

41. As per discussion in time stamping.

Costs associated

42. As per discussion on time stamping.

Assessing solutions against the OECD's electronic commerce guiding principles[15]

43. From the above discussion the only options which appear to improve the integrity of electronic documents are time stamping and notarisation. As these solutions are virtually identical for the purposes of this section we will refer to them as being the "solution".

Neutrality

44. The solution breaks the principle of neutrality in that it requires electronic documents to be attested by an independent third party. This only occurs in the "physical world" in very limited circumstances.

Efficiency

45. The solution is reasonably efficient in its design and delivery.

Certainty and simplicity

46. The solution goes some way to providing certainty as to the integrity of electronic documents.

---

14. See ISO SC 27 Standing Document no 6 "*Glossary of IT Security Terminology"* available from http://www.jtc1.org

15. For further details on the OECD's guiding principle on electronic commerce refer to document titled *Electronic Commerce: Taxation Framework Conditions* available at www.oecd.org

Effectiveness and fairness

47. While the solution may be characterised as being effective it can not be held to be fair as it places additional costs on businesses who choose to function in this manner.

Flexibility

48. No requirement to assess against this criteria.

Conclusion / Where to from here

49. Ideally what is required is for commercial and inhouse accounting systems (plus other tax relevant systems) to produce and maintain data in a form that:

a) Is encrypted with sufficient security maintained over the key to ensure others can't access the system or alter the data.

b) Data is "time stamped" by the creating system at the time of creation plus at the time of any alteration; and

c) Alterations to leave an audit trial of:

- When the original was created.
- Original content; and
- Change register showing what has changed, by whom, when and for what reason.

ANNEX XX:
PROVING THE TIME OF TRANSACTION OCCURRENCE[1]

1. Merchants who use computer based transaction management systems anchored off a database usually have a built in time utility. Because of the need to properly order transactions, based on sequence, there is a mechanism which places relative times on data entries. The times are anchored from the system clock. These time stamps were not meant to establish absolute time, but rather time relative to other data entries. While perhaps not accurate to the second they are easily within the "day" accuracy which government representatives have indicated is the critical time frame.

2. Databases can be cross referenced to atomic or trusted time for greater accuracy.

Timestamps are digital watermarks

3. To speak generally first, assuming sufficiently strong cryptography is used, timestamps serve as a digital watermark whereby a digital event is sealed and can be proven what-it-was-at-that-moment so long as the timestamp is stored/archived. Based upon the way time is input into the enterprise will determine whether the timestamp is portable, that is, whether and to what extent other enterprises will trust the timestamp and the representations it contains.

4. For more general information on time and the requirements around trusted time, and for a free synchronisation client that will allow to you "set" your pc clock, please see the white paper attached that details the nature of timing devices and the problems inherent in attempting to prove the time within the enterprise using the most prevalent methods available, and visit www.certifiedtime.com.

Outsourcing time management to a trusted timing authority

5. CertifiedTime, Inc. (CTI) is able to instil trusted time within the enterprise. We do this in response to synchronisation requests from licensed devices by establishing a chain of command over time-data from NIST monitored-and-certified timeservers housed at a Certified Timing CenterTM and delivered over a private circuit to the requesting device which is thereby synchronised to UTC(NIST).

6. The timing request and successful (or unsuccessful, if such) synchronisation is logged and securely archived at the CertifiedTime Data Center. Synchronisation requests can be done several, dozens, hundreds or even thousands of times per day as necessary, depending on the trust parameters and audit requirements controlling the requesting device. For example, a PC or trader workstation might need to be synchronised every ½ hour, while a firewall router might be synchronised every 5 minutes.

7. By instilling trusted time into the enterprise, the enterprise can then issue its own trusted timestamps, using its own preferred timestamping protocol. And the real value of this is in the portability

1. CertifiedTime is a vendor of timestamping services that has been asked to provide technical expertise on timestamping; CertifiedTime materials are provided for information and are not meant to be an OECD endorsement.

of that trust -- by using an authentic and authorised source of time, NIST, to anchor the time base, using CTI's evidentiary grade time, other enterprises can trust the timestamps generated. This aspect of the service is an outsourcing of time management services.

8. Within an enterprise, timestamping can be more securely archived for audit purposes by developing a procedure to create a daily hash of the transaction record. One should be aware that this still may be a burden for businesses involved in high volume transactions. It is also unclear whether such archives are needed if current, trustworthy back-end procedures are already in place.

9. Depending on business models and information architecture, applications may be the more appropriate place to engage Timestamping technology. Not all information which may be part of a database may need to have trusted time trails. Applications utilising verifiable time technology can be a more selective and less resource intensive way of creating a trusted time environment.

Outsourced time stamping authority

10. Should the enterprise desire, it can outsource the timestamping as well whereby CTI or some other trust services provider can act as a Time Stamping Authority. This would alleviate the enterprise of selecting or devising a timestamping protocol, and the burden of storing and archiving all timestamps for all recorded transactions. However, to create a trusted audit trail, either the enterprise or the Time Stamping Authority selected would have to be able to prove the time being used, so they would most likely have to have trusted time installed, too.

Business rationale

11. While a number of companies may have a business rational for using trusted time mechanisms, this will not apply to all business, and will be much less critical for SMEs engaged in retail transactions. Based on discussions at the joint PDA/Tech TAG meeting those businesses were the area of greatest concern because of the lower probability of established back end procedures and audit oversight. Conversely it was assumed that large companies had sufficient procedures and audit oversight to provide comfort in accepting transaction reports. It should also be noted that reliable trusted time systems are just now emerging which means that even the majority of larger companies will not have had the opportunity to evaluate the need or applicability of this technology to their business models.

12. It is also important to check the reality of concerns related to reliability of e-commerce systems in SMEs. The overwhelming majority of SMEs do not make decisions related to software components or hardware architecture. There is no expertise for these decisions within SMEs, they rely on consultants or end-to-end solution vendors to deliver both turnkey systems and needed support/maintenance. While system clocks are not guarded by internal security from the systems owner, and the ability to change such a clock does not present a significant technical challenge, SMEs are usually sufficiently challenged by just keeping the system on and entering the information properly.

13. It is arguable that the small percentage of SME which may be inclined to hide income would be more likely to try to input incorrect information - a mirror of how this would be accomplished in the paper world. If that assumption is correct, electronic systems may actually be more reliable because they try to build in safeguards to prevent the input of erroneous information - not to prevent fraud but rather to avoid inadvertent error. The majority of bad actors (who wish to cheat on income from transactions) would probably shy away from electronic systems because they would feel less control of the system. It is more

difficult to architect two sets of books online when one has no experience with computers. Off line fraud only requires mastery of a writing instrument and adding machine.

14. However, an intimate knowledge of how to manipulate computer systems is not required where unscrupulous software programs, such as “zapper” are developed. These programs are specifically designed to falsify records and hide certain transactions. News of these techniques generally spreads rapidly through an industry, especially traditional cash based industries. Tax authorities will have to be attuned to new tools to defeat the integrity of systems much as they must keep abreast of new tax dodges and schemes for illegally sheltering income. Tax authorities must also make sure that they have audit experts that are experienced in online business methods and models. They must catalogue and understand the digital footprints that electronic records leave and develop compliance models for online business types that provide a basis for comparison across tax paying entities.