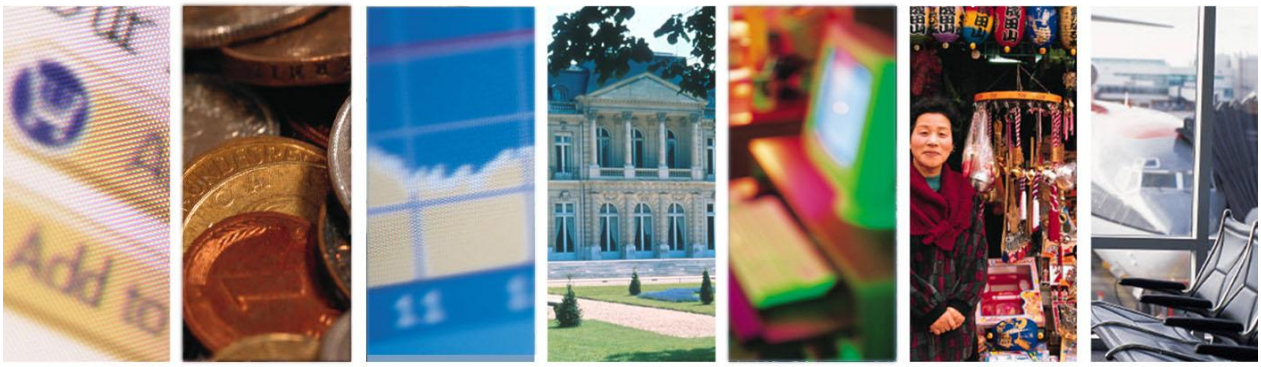
ORGANISATION FOR ECONOMIC CO-OPERATION AND DEVELOPMENT

ORGANISATION DE COOPÉRATION ET DE DÉVELOPPEMENT ÉCONOMIQUES



FORUM ON TAX ADMINISTRATION: TAXPAYER SERVICES SUB-GROUP

Security and Authentication Issues in the Delivery of Electronic Services to Taxpayers

January 2012

TABLE OF CONTENTS

Boxes

Tables

Graphs

Annexes

ABOUT THIS DOCUMENT

Purpose

This report summarises the findings of a survey conducted by the Forum on Tax Administration's Taxpayer Services Sub-group to assess and provide a comprehensive picture of the major security and identity authentication issues faced by member countries in delivering e-services, and the solutions implemented or planned.

Background to the Forum on Tax Administration

The Forum on Tax Administration (FTA) was created by the Committee on Fiscal Affairs (CFA) in July 2002. Since then the FTA has grown to become a unique forum on tax administration for the heads of revenue bodies and their teams from OECD and selected non-OECD countries.

In 2009, participating countries developed the *FTA vision* setting out that……. *The FTA vision is to create a forum through which tax administrators can identify, discuss and influence relevant global trends and develop new ideas to enhance tax administration around the world.*

This vision is underpinned by the FTA's key aim which is to……. *improve taxpayer services and tax compliance – by helping revenue bodies increase the efficiency, effectiveness and fairness of tax administration and reduce the costs of compliance.*

To help carry out its mandate, the FTA is directly supported by two specialist Sub-groups—Compliance and Taxpayer Services—that each carry out a program of work agreed by members. Both OECD and selected non-OECD countries participate in the work of the FTA and its Sub-groups.

The Taxpayer Services Sub-group exists to provide a forum for members to share experiences and knowledge of approaches to taxpayer service delivery, in particular through the use of modern technology. To achieve this objective, the Subgroup's mandate calls for it to:

1) Periodically monitor and report on trends in taxpayer service delivery, with a particular focus on the development of electronic/online services;
2) Examine ways to promote the uptake and use of electronic services by revenue bodies;
3) Examine options for cross-border administrative simplification and consistency; and
4) Assist, as appropriate, other groups of the CFA.

Caveat

National revenue bodies face a varied environment within which to administer their taxation system. Jurisdictions differ in respect of their policy and legislative environment and their administrative practices and culture. As such, a standard approach to tax administration may be neither practical nor desirable in a particular instance.

The documents forming the OECD tax guidance series need to be interpreted with this in mind. Care should always be taken when considering a country's practices to fully appreciate the complex factors that have shaped a particular approach.

Inquiries and further information

Inquiries concerning any matters raised in this information note should be directed to Richard Highfield (CTPA, International Co-operation and Tax Administration Division) at e-mail Richard.highfield@oecd.org

GLOSSARY OF TERMS

Access Token	A method used to identify a taxpayer or intermediary for use in connecting to secure electronic services for example a password or a digital certificate.
Biometrics	Method for uniquely recognising a taxpayer based upon one or more physical characteristics for example: fingerprint, voice, iris recognition, face recognition
Code Card	A card containing a large number of paired codes. The tax administration will challenge the taxpayer with one of the pair and the taxpayer must respond with the matching code of the pair.
Data Confidentiality	Assurance that data transmitted (in both directions) remains confidential.
Data Integrity	Assurance that what was received was exactly what was sent (both directions)
Data Non-repudiation	Assurance that the identified sender cannot deny that the exact item received was in fact the same item sent by the identified sender (both directions)
Digital Certificate/Digital Signatures/PKI	PKI – Public Key Infrastructure – basically this is a security protocol that uses a pair of 'keys', one normally held by the taxpayer (not always the case) and the other by the administration. A taxpayer uses their key to log in, sign and submit information which is compared against the key held by the administration. Both must match in order for data to be accepted or for the user to be allowed access to the tax administration's secure services. A digital certificate or digital signature fulfils the same function.
Identity Authentication	Assurance as to the identity of the person or his/her intermediary who transacted the data (both directions) or accessed confidential taxpayer data.
Hashing Data	A hash function is used to encrypt data by applying an algorithm with some seed values to scramble the data, which also allows the data to be later, decrypted with a certainty that the data has not been changed in anyway. This function can also be used to encrypt data for confidentiality.
Out-of-Band	Out-of-Band is the use of two or more separate communications channels communicate different parts of the registration process to the taxpayer e.g. Internet to apply for registration, password issued by land mail. This enhances the security of the registration process
Shared Secrets	Challenging the taxpayer to reveal information that only the Revenue authority and the taxpayer should know, usually information contained in the taxpayer's tax records
SSL encryption	Secure Sockets Layer SSL is a software system that encrypts the network connection between the Revenue and the Taxpayer. This ensures that the data passing in either direction remains confidential. SSL is used worldwide for assuring the confidentiality of internet transactions.
Tax Intermediary	Within this report, the term tax intermediary includes any person acting for and with the approval of a taxpayer, and meeting any criteria required by the tax administration or by legislation in a given territory. This includes all persons known in different contexts and jurisdictions as taxpayer representative, tax agents, tax practitioners, tax consultants etc.

SUMMARY

Governments, and particularly revenue bodies, are relying increasingly on electronic services to improve customer services while at the same time reducing costs. However, with the widespread adoption of electronic services in the delivery of customer services in many aspects of everyday life, customers and service providers alike have experienced an exponential growth in the frequency and sophistication of criminal attack. Taxpayer services are no exception to this, and revenue bodies must be constantly vigilant to mitigate the risks associated with identity theft, financial loss and reputational damage caused by attack on the electronic service channels. Revenue bodies must also be constantly vigilant to mitigate the risks to compliance arising from taxpayers who may exploit weaknesses in the legal strength of identity authentication and non-repudiation systems to deny transactions or transaction contents in order to escape penalty or prosecution. Society, the media, and individual and corporate taxpayers understandably expect government services to be secure, and security and identity authentication are key aspects of this risk mitigation, yet a careful balance has to be made to ensure the safeguards put in place do not themselves become a barrier to take-up of the service.

Drawing on a survey of 25 revenue bodies, this report describes aspects of their security and authentication framework and provides a comprehensive picture of the major data security and identity authentication issues being faced by member countries in delivering e-services, and the solutions implemented or planned. The key findings are as follows:

Key Findings

- ***Overall developments.*** It is noteworthy that despite the steady growth in the range and uptake of electronic services in taxpayer services, the most widely used security and authentication technologies have remained largely unaltered over the past decade. The issues surrounding the management and maintenance of many of these –digital certificates, PIN numbers, passwords, tokens and code cards– are well known by all revenue bodies, yet at present there still appear to be few established alternatives. The current experience with new technologies which offer the promise to prevent or reduce these issues –such as biometrics, or the use of cloud computing in areas such as the management of digital certificates– is very limited, but these innovations are just appearing on a small number of revenue body agendas, and may warrant investigation to update this report once they have become more mature.
- ***The national context.*** A significant majority of revenue bodies (80%) benefit from the existence of a national identity register to aid them in identity authentication. A smaller percentage (48% with an additional 20% planned) go further and provide a national identity authentication service, enabling government departments and agencies to share the benefit of a service built once rather than many times within a country. This reduction in complexity also reduces the administrative burden of compliance, which is a strategic goal in many revenue bodies. This whole-of-government approach offers significant benefits to both the service provider and its customers.
- ***Third party authentication services.*** A significant minority of countries (48%) use a trusted third party authentication service. A number of valuable benefits are reported, and no issues were reported related to the fact that the authentication service was provided by a third party.
- ***First registration with the tax authority.*** Almost all countries use identity proof information from a national or private third party identity register for new taxpayer registrations, and the requirements generally vary by customer group.
- ***Channels used.*** The Internet is by far the most widely used channel. For **existing services**, the Internet is used for 562 service offerings (out of a potential 800 considered by this study) and is the most mature; telephone (voice) at 158 and secure email at 136 are at the second highest level of maturity; IVR at 69 is relatively immature; and telephone (SMS) and intelligent mobile devices at 19 and 8 respectively are both quite embryonic. Although used for 61 service offerings, standard email can be considered mature but of limited use in the context of secure electronic interactions. For **planned new services**, the picture is quite different, with 39 new service offerings planned for intelligent mobile devices, 36 for secure email, 20

for telephone (IVR), 16 for telephone (voice), 12 for the Internet, and none for either telephone SMS and standard email. However, if these planned new service interactions are all implemented over the course of the next two years, they will have a relatively modest impact overall on the significance of the various channels in the strategies of the participant revenue bodies with two exceptions: secure email will become as significant as telephone (voice) as the tie second most important channel; and the use of telephone (SMS) will fall below intelligent mobile devices into the position of channel of least significance.

- ***Identity authentication methodology.*** The primary identity authentication methodology in use by most revenue bodies has a common pattern to it i.e. effectively establish the identity of the taxpayer or tax intermediary from the outset, and issue an access token to the identified taxpayer or intermediary for use in connecting to secure electronic services.
- ***Accessing services.*** There is considerable consistency regarding the **technology (tokens)** used for accessing the secure services. The most common systems/tokens used are one or a combination of the following: Digital Certificate, User ID, PIN and Password. Other tokens used include Code Card, Electronic ID card, Shared Secrets/tax records and National ID. Although digital certificates are regarded as the most secure method for assuring the identity of a taxpayer some revenue bodies are re-considering their continued use of digital certificates, on the basis of their negative impact on the uptake of electronic services, combined with the relatively high cost of administering them. The identity authentication provided by Password, PIN shared secrets etc is considered by many administrations to be perfectly adequate for assuring identity for most –if not all– secure electronic services, and there is evidence of some administrations shifting to this authentication method from digital certificates or planning to do so. Only three respondents reported that they used biometrics as part of their identity authentication, and the use of this technology should be considered quite embryonic in this context.
- ***Services offered to main customer groups.*** In terms of the services offered to the four customer groups studied (employees, business corporate, business individual and tax intermediary), there is remarkably little variation in the total number of service offerings to each of the customer groups.
- ***Data confidentiality.*** Almost all respondents use the common widely used SSL data encryption or equivalents to assure data confidentiality for data exchange by internet. This SSL system continues to provide the best solution for tax administrations.
- ***Data integrity.*** Data integrity is mainly assured by hashing the data. In general, the majority of respondents indicated hashing to be of at least adequate strength. Digital Signatures using Public Key Infrastructure (PKI) can also be used to provide data integrity checks.
- **Non-repudiation.** There is more variety in responses in relation to assuring data non-repudiation. Replies included using digital certificates, database logs, terms and conditions or shared secrets. The overall strength of these methods is considered by respondents to be at least adequate.
- ***Legal frameworks.*** Most countries (84%) have legal frameworks supporting identity authentication, and slightly higher (92%) have legal frameworks supporting data confidentiality. In most cases the legal framework involves a combination of national and tax legislation, as well as policies and procedures operated by the tax administration. In many cases the main differences in the ways administrations implement identity authentication and data security have more to do with differences in the laws, policies and the cultural and political drivers in place concerning privacy and data security rather than technical constraints or usability issues.

Recommendations

- *Adopt a whole-of-government approach where feasible:* Revenue bodies should support government services or plans for the establishment of national identity registers and national identity authentication services, and make full use of these where they exist.

- Revenue bodies not able to use a government national identity authentication service may wish to consider the use of a trusted third party service. This report provides details of which other countries have successfully adopted this approach, and of the benefits which they have identified.
- Revenue bodies should continue to monitor both customer demand and channel maturity for electronic service delivery in other sectors, as the relative significance of the different channels could change quite markedly even over the short and definitely over the medium term.
- Revenue bodies reviewing their own channel strategy or technology strategy for the delivery of secure electronic services should consider liaising with peers –identified in this report– who have already adopted the aspects they are considering, especially (with respect to technology strategy) in relation to digital certificates and biometrics.

I. BACKGROUND

1. Governments, and particularly revenue bodies, are relying increasingly on electronic services to improve customer services while at the same time reducing costs. However, with the widespread adoption of electronic services in the delivery of customer services in many aspects of everyday life, customers and service providers alike have experienced an exponential growth in the frequency and sophistication of criminal attack. Taxpayer services are no exception to this, and revenue bodies must be constantly vigilant to mitigate the risks associated with identity theft, financial loss and reputational damage caused by attack on the electronic service channels. Revenue bodies must also be constantly vigilant to mitigate the risks to compliance arising from taxpayers who may exploit weaknesses in the legal strength of identity authentication and non-repudiation systems to deny transactions or transaction contents in order to escape penalty or prosecution. Society, the media, and individual and corporate taxpayers understandably expect government services to be secure, and security and identity authentication are key aspects of this risk mitigation, yet a careful balance has to be made to ensure the safeguards put in place do not themselves become a barrier to take-up of the service.

The role and work of the Forum

2. At its June 2010 meeting, the FTA Bureau considered a proposal from the Taxpayer Services Sub-group to conduct a study to assess and provide a comprehensive picture of the major security and identity authentication issues faced by member countries in delivering e-services, and the solutions implemented or being planned. It decided that security and authentication were key aspects of the effective and secure delivery of electronic services, which themselves are a key aspect of many revenue bodies' business strategies. In view of the risks related to the pace of technology change, incidence and frequency of attempted criminal attack or abuse by taxpayers, potential financial losses, media and public concern, and potential reputational damage if a revenue body's electronic services were to be compromised, it agreed that a study on security and authentication in electronic services should be undertaken. It tasked the Taxpayer Services Sub-group to conduct this study.

Prior work of the Forum and security and authentication issues

3. At the Taxpayer Services Sub-Group meeting held in October 2010, members reviewed the results of the '2009 Survey of Trends and Developments in the Use of Electronic Services for Taxpayer Service Delivery' to identify specific areas that would benefit from a more focused examination as part of the future work plan. The survey had been undertaken to assess member revenue bodies' progress with, and plans for, the use of modern technology to provide services to taxpayers. Aspects of security, specifically authentication, were included within the survey's scope.

4. A key finding of the survey was that security matters, particularly issues concerning taxpayers' authentication, were an ongoing concern for most revenue bodies. A large number of solutions were being used in member countries (primarily User ID / Password and digital certificates) and many revenue bodies had plans to either simplify, or make more secure, access to and use of electronic services.

5. A suitable security solution requires a balance between security (ensuring the level of control is appropriate to the sensitivity of data being accessed) and usability (ensuring the security solution is not so annoying that it drives users away). The study examined the experiences of tax administrations in their attempts to achieve an adequate balance between quality service and security.

6. Also discussed at the October 2010 meeting:

    - The need for different techniques and levels of authentication, depending on the user channel (telephone or Internet) and the sensitivity of the service provided. (A study could examine the different security levels required to meet the needs of different communications channels and how these different security levels can co-exist harmoniously;

- The possible consequence of the increasing use of mobile phone technology and the emergence of whole-of-government portals in the evolution of security and authentication solutions; and
- The broader issue of securing incoming data (e.g. tax returns filed electronically via Internet) and outgoing data (e.g. tax notifications sent electronically to taxpayers).

7. In their discussions, members acknowledged that ensuring confidentiality, integrity and non-repudiation in such electronic processes involves legislative aspects and security mechanisms such as digital signature, which appear to vary considerably across member countries

The study

8. The objective of this study was to provide a comprehensive picture of the major security and identity authentication issues faced by member countries in delivering secure electronic services, and the solutions implemented or planned, in order to draw possible trends and provide recommendations to revenue bodies, depending on the context they face.

9. As elaborated later in this note (see Box 1), "Identity Authentication" refers to the establishment of a successful link between an assertion of "who I am", with an accepted method of proof – "how can I prove it". In the context of this report, "Security" refers to the safeguards put around what successful identity authentication allows me to do. Both identity authentication and security can be considered as services, and this report also covers the legal frameworks underpinning these services.

10. The study was conducted by means of a detailed questionnaire issued to all members of the Taxpayer Services Sub-group. The study team, led by Ireland and also comprising Australia, Belgium, Chile, France, Germany, Ireland, New Zealand, Norway, Portugal, Spain and Sweden worked with the OECD Secretariat to develop both the scope document and also the outline and detail of the survey questionnaire, which was forwarded to all members of the Taxpayer Services Sub-group in December 2010. Twenty-five survey responses were received, which were followed up where necessary with specific questions, and the information gained forms the basis for the analysis and commentary contained in this report.

Approach to the study

11. The potential scope for a study in this area is very broad. Accordingly, the approved scope document for this study defined the scope to cover three main topics:

    1) Taxpayer identity authentication;
    2) Securing data/documents exchanges; and
    3) The legal frameworks underpinning these services.

12. Furthermore, the study confined itself to an examination of the security and identity authentication issues attaching to electronic services that provide for any transaction exchange, in either direction, between the administration and a taxpayer, or taxpayer representative[1], which alters confidential taxpayer data or provides access to confidential taxpayer data.

Taxpayer identity information

13. In taxpayer identity authentication, the different security levels commonly defined by tax administrations were examined to determine how they match the different taxpayer services delivered online or via other electronic channels. An inventory was compiled of the different

[1] Within this report, the term taxpayer representative includes any person acting for and with the approval of a taxpayer, and meeting any criteria required by the tax administration or by legislation in a given territory. This includes all persons known in different contexts and jurisdictions as tax intermediaries, tax agents, tax practitioners, tax consultants etc.

identity authentication solutions [2] currently in use (or planned for the near future) to authenticate taxpayers (both individuals and businesses) for each security level: password-based, digital certificates using different devices or biometric methods (the latter was shown to remain unimplemented by tax administrations in the "2009 survey of trends…"). The ways that administrations authenticate the identity of a taxpayer at the time that a tax identity is originally issued were examined, as well as the ways that administrations implement identity authentication for their electronic services. Finally, the drivers that led countries to choose one authentication method over others were considered, including strength of authentication and ease of use considerations.

Securing data and document exchanges

14. In securing data and document exchanges, both incoming data/documents (such as tax returns electronically filed by taxpayers) and outgoing data/documents (such as tax notifications sent electronically to taxpayers) were examined, relating to the communications channels which were confined to those described in paragraph 16 below. The study reviewed the methods and solutions adopted (or planned) by tax administrations to secure documents electronically exchanged between tax administrations and their taxpayers –i.e. ensuring confidentiality, integrity and non-repudiation.

The legal frameworks

15. The legal frameworks and certificate policy and practice statements were considered which are in use and tested in administrations that provide a legal framework to support: authentication – prosecution strength assurance as to the identity of the person or his/her agent who transacted the data; confidentiality –robust data protection assurance that transmitted data remains confidential; data integrity– prosecution strength assurance that what was received was exactly what was sent; and non-repudiation – prosecution strength assurance that the identified sender cannot deny that the exact item received by the revenue body was in fact the same item sent by the identified sender.

Other considerations – channels, key services, taxpayer groups and risks

16. The specific channels that were examined were 1) the Internet; 2) email – including standard email and secure email; 3) telephony – including voice, short messaging (SMS) and Interactive Voice Response (IVR); and 4) intelligent mobile devices (e.g. iPhone, iPad, mobile devices using 'android' technology).

17. The report also examined eight typical and widely provided services of revenue bodies, across four main taxpayer groups. The categories of taxpayer service examined were: 1) view tax account information; 2) file a return; 3) amend return details; 4) amend taxpayer basic information; 5) make a payment; 6) claim repayments / credits / allowances; 7) submit bank account details; and 8) access confidential information sent by the revenue body. The four main taxpayer groups were: 1) business corporate; 2) business individuals; 3) employees; and 4) tax intermediaries.

18. Risks were considered under the following headings:

    - Identity authentication: Assurance as to the identity of the person or his/her intermediary who transacted the data (both directions) or accessed confidential taxpayer data.
    - Data integrity: Assurance that what was received was exactly what was sent (both directions;
    - Non-repudiation: Assurance that the identified sender cannot deny that the exact item received was in fact the same item sent by the identified sender (both directions); and
    - Confidentiality: Assurance that data transmitted (in both directions) remains confidential.

[2] The term "solution" is interpreted with a broad meaning, covering both the technical solution and the process in place to deliver the authentication solution (e.g. how shared secrets are delivered to the taxpayer, how digital certificates are acquired by the taxpayer or a third party user…).

This report

19. The report is structured as follows:

- Chapter II provides the strategic context—key factors that are influencing the development of security and authentication arrangements;
- Chapter III provides a comprehensive picture of the major identity authentication methods used by member countries in delivering e-services, the issues they face and the solutions implemented or planned, in order to draw possible trends and provide recommendations to revenue bodies, depending on the context they face.
- Chapter IV provides a comprehensive picture of the methods and solutions adopted (or planned) by tax administrations to secure information electronically exchanged between tax administrations and their taxpayers – i.e. ensuring confidentiality, integrity and non-repudiation.
- Chapter V provides an examination of the legal frameworks and certificate policy and practice statements, in use and tested by revenue bodies that provide a legal framework to support identity authentication, data confidentiality, non-repudiation and data integrity.
- Chapter VI sets out key findings and recommendations from the work undertaken.

II. STRATEGIC CONTEXT FOR THE STUDY

20. The Forum's interest in security and authentication matters at this time arises in large part from three factors:

    - Rapid growth in the range of services being offered to, and used by, taxpayers, particularly services involving the exchange of personal data, has intensified the need for revenue bodies to have robust and, at the same time, security and authentication mechanisms that are easy to use;
    - Technology advances are presenting new opportunities for enhancing the way government services can be delivered, applying a more citizen and business centric approach to how services are designed and delivered; these new opportunities, termed 'whole-of-government' approaches dictate the need for a common and secure sign-on capability that can be readily and easily applied by the clients of participating government agencies.
    - Technology advances are also exposing revenue bodies increasingly to a range of external threats, particularly by perpetrators with fraudulent conduct in mind.

Growth in the nature and use of electronic services by taxpayers and tax intermediaries

21. The Forum's report '*Survey of Trends and Developments in the Use of Electronic Services for Taxpayer Service Delivery*' [3] published in March 2010 noted the significant progress being achieved by many revenue bodies in their delivery of electronic services to taxpayers and tax intermediaries. In particular, it highlighted:

    - Significant growth in the use of e-filing and e-payment services by taxpayers and tax intermediaries, in many countries now being the predominant means adopted by taxpayers for interacting with the revenue body;
    - The emergence of new more personalised products (e.g. prefilled tax returns) that can be accessed online by taxpayers and their authorised representatives;
    - The provision of personal taxpayer data via the Internet to taxpayers and their authorised representatives;
    - Growth in the use of call centres (and related work volumes) and the emergence of mobile telephony as a service delivery medium; and
    - The early emergence of 'whole-of-government' service approaches (e.g. government portals, common business and citizen registration and numbering systems), including single 'sign-ons' in a few countries for authentication purposes.

22. Looking to the future, it noted that the plans of most revenue bodies' signalled further increases to the range, quality, and take-up of their Internet-based services as their number one priority.

Whole-of-government service delivery approaches

23. The Forum's 2010 report also observed that while developments with 'whole-of-government' approaches still appeared relatively immature, putting all of the developments observed together to form a picture of a possible future clearly pointed to 'whole-of-government' approaches representing the next paradigm in government service delivery. This future paradigm had been the subject of complementary work done by the Forum and is described in the note *'Framework for the provision of e-services*', also published in March 2010. Specifically, this future state – denoted in the report as 'Phase 4 – integration or transformation' – was described in the following terms .....

[3] See www.oecd.org/document/60/0,3746,en_2649_33749_45037436_1_1_1_1,00.html

"This phase is characterised by a seamless interface and integrated service delivery model in which the relationship between communities, government and business has been transformed. Multiple channels of service delivery are a given and new means of service delivery are being continuously explored. The mechanisms of e-government are taken for granted as part of everyday life and e-government as a concept effectively 'disappears' to become simply 'government'. Citizens and business have an implicit trust and confidence in their engagement with government, and the concept of 'government as a servant of the public' is truly realised as personalised, pro-active service delivery mechanisms abound. The distinctions between agencies at all three levels of government (local, state, federal) are notional as collaborative service delivery is not only the norm, but a means of achieving and delivering previously un-conceived levels of service. Government services are fundamentally personalised, independent of channel of delivery or service provider and frequently transparent. Government itself is highly accountable, and the mechanisms for soliciting feedback from communities have been replaced by mechanisms that afford communities a highly participative role in decision-making, direction and policy.

Key dependencies for this phase include:

- *Agency collaboration to develop integrated, customer-driven processes requiring the re-engineering of all business processes. It will be particularly important for governments to "virtually" unify existing customer service centres so that all customer/constituent contact can be identified to the customer of record and transformed into standard input to state workflow. The goal should be to work toward the development of an automated enterprise workflow.*

- *The e-implementation of new applications data structures developed based on the notions of client-centricity, shared services, and shared infrastructure."*

Security and privacy threats

24. The 2010 report also noted that e-government strategy statements developed by a number of advanced economies give emphasis to the criticality of appropriate security and privacy protection safeguards. For example, Denmark's strategy called on public sector agencies to guarantee continued safe and secure handling of data in the public sector, while the EC's note emphasised the need for a specific risk management approach to these matters. In relation to tax administration, the report highlighted the concerns in this area of one of the largest revenue bodies in the FTA, expressed in the following terms.....

"*Technologically savvy employees and taxpayers are demanding that government institutions provide them the same level of tools and online capabilities as best-in-class private-sector organizations.*

As more people gain access to the Internet, and as IT systems become more inter-connected, data security concerns rise. Safe-guarding data and systems today are much more difficult than it was a few years ago. Data vulnerability is exacerbated by the fact that criminals are increasingly focused on accessing personal financial information. In fact, attempts at identity theft and phishing (i.e., online scams to steal personal data) related to federal income taxes increased more than sevenfold in 2008.

We must become more technologically sophisticated to meet increased taxpayer expectations and maintain data security – modernizing our systems, improving our training, and continually enhancing our safeguards (USA IRS 2009-2013 Strategic Plan).

III: TAXPAYER IDENTITY AUTHENTICATION

25. Revenue bodies typically provide much information and guidance of a general nature to taxpayers. This information is not unique to any taxpayer and is not sensitive, and generally under these circumstances, identity authentication is not necessary.

26. Increasingly though, revenue bodies and taxpayers wish to interact with each other electronically or via the telephone to conduct taxpayer unique interactions. The tax affairs of individual taxpayers and business whilst in discussion are invariably confidential, and even after year end finalisation they remain confidential in most countries. To ensure this confidentiality, as well as to ensure against inadvertent errors and malicious attack, effective identity authentication is essential. The following table illustrates the high level principles of how this is achieved.

Table 1. Aspects of Identity Authentication

	Provided by	Answers	Attributes
Identity	principal	"Who are you?"	public assertion
Authentication	principal	"OK, how can you prove it?"	secret response
Authorization	system	"What can I do?"	token or ticket
			access control

Source: Microsoft TechNet

27. This section of the report provides a comprehensive picture of the major identity authentication methods used by member countries in delivering secure electronic services, the issues they face and the solutions implemented or planned, in order to draw possible trends and provide recommendations to revenue bodies, depending on the context they face.

28. The Identity Authentication part of the study examined the following topics:

- Identity authentication: national context:
  - National identity register and national identity authentication services
  - Private trusted third party identity registers and identity authentication services
- Taxpayer and tax intermediary registration with the Tax Administration:
  - Identity authentication: taxpayer first registration with the revenue body
  - Identity authentication: tax intermediary first registration with the revenue body
  - Linking of taxpayers with their tax intermediary on the administration's records.
- Channels of communication:
  - Identity authentication: internet services
  - Identity authentication: secure e-mail services
  - Identity authentication: standard e-mail services
  - Identity authentication: telephony voice services
  - Identity authentication: telephony SMS/text services
  - Identity authentication: telephony IVR services
  - Identity authentication: intelligent mobile device services

Identity authentication: national context

29. As described in Chapter II, which referenced the key conclusions of the 2010 report "Survey of Trends and Developments in the Use of Electronic Services for Taxpayer Service Delivery", following a "whole-of-government approach" and enabling a single sign-on to government services was one of the areas receiving attention in a number of countries, when the study for the survey report was conducted in 2009. This "single sign-on" is in practice achieved through the provision of a single identity authentication service facilitating and safeguarding access to all government services.

30. The increase in the maturity of e-government services to the citizen and to business can have a significant influence over how a tax administration provides its own services to the taxpayer. Choices by the tax administration concerning the implementation of identity authentication and the data exchange security requirements can be greatly influenced by the national implementation of cross-government secure services to the citizen and to business.

31. This area of the study sought to examine the national contexts in which tax administrations operate and describe the strengths and weaknesses of being part of an e-government implementation of identity authentication. The national context part of the study examined the following:

    - The availability and use of national identity registers and national identity authentication services; and
    - The availability and use of private trusted third party identity registers and private trusted third party identity authentication services.

32. The legal frameworks in place to support identity authentication, personal data protection and commercial data protection are examined in Chapter V of this report.

National identity register and national electronic identity authentication services

33. This area of the study explored how tax administrations implement national identity registers and national electronic identity authentication provided by a national authority (e.g. central government) and the issues that this type of service raises. The survey posed the following questions (the detailed revenue body responses to which can be found in Annex 1):

    1) Do you have a national identity register run by central government or a government department?
    2) If not, why do you not have a national identity register?
    3) What identity proofs are required for individuals when registering on your national identity register?
    4) What identity proofs are required for business when registering on your national identity register?
    5) If you have a national identity register and you do not use the service, why not?
    6) What are the benefits to your tax administration from having a national identity register?
    7) Does the tax administration supplement the national identity register with its own additional data? If yes, why?
    8) Is a national electronic identity authentication service provided for your tax administration? If yes, how does this operate?
    9) Does the national electronic identity authentication service satisfy all the identity authentication needs for all your tax administration electronic services? If not, what tax services does it not support, and why?

34. The key findings of an examination of the impact that national identity registers and national electronic identity authentication services have on revenue bodies (see Table 2) are set out hereunder:

National identity register

- The majority of the respondents (20/25, or 80%) indicated that there was a national identity register in place in their jurisdictions, and there was common agreement that there are significant benefits to be gained by a tax administration from having a national register in place, with no weaknesses identified.
- Across surveyed bodies a variety of benefits from having a national identity register were identified, including the following:
    - Provides an authoritative and certified source of identity data;
    - Provides efficiencies in assisting the identification of taxpayers;
    - Reduces administrative work;
    - Avoids replication;
    - Facilitates the sharing of identity information between different departments and public bodies;
    - Facilitates the re-use of data;
    - Reinforces the mechanism for identity proof and standardises the process;
    - Provides an additional security level; and
    - Customer service benefits were also noted, such as avoiding the need to contact taxpayers and providing a simpler and more streamlined system for taxpayers and revenue bodies.
- Of the five countries that do not have a national identity register, three indicated that the reasons for not having a national identity register were influenced by factors such as a strong privacy culture (Australia) – where they have a national identity register for business, but for privacy reasons, not for individuals, and a strong belief in data protection (Germany), as well as political sensitivity (USA). In Germany, although national law does not allow a centralised national identity register of individuals, local identity registers are managed by local authorities /communities and data from these registers are sent to the central tax office; business registers are managed by local courts.
- Across surveyed bodies there was limited variation in the type of identity proofs required for individuals when registering on national identity registers. The proofs most commonly required included the following items: photo identification, passport, personal /national identification card and registration at birth or registration from a birth certificate.
- Survey responses indicated that in many countries the business register in place is managed separately to the individual identity register. In three cases (Germany, Spain and Mexico) respondents advised that there is no national business register, but rather the register is managed at a local level.
- Of the respondents that provided details of the identity proofs required for business in their jurisdiction, in most cases the identity proofs involved some form of personal identification of the person submitting an application for inclusion on the business register, or of representatives, or, in some cases, of the Chief Executive Officer (CEO) and board members (for instance, photo identification, signature). In most cases proof concerning the establishment of the business is also sought.
- Among the respondents who reported that there was a national identity register in place, the majority (13/19) noted that the tax administration supplemented the national identity register with its own additional data, four respondents noted that they did not supplement the national identity register, while one country (Estonia) advised that it planned to do so.

National electronic identity authentication service

- Just under half of respondents (12/25 or 48%) advised that they have a national electronic identity authentication service provided for their administration, with a further 5 of the 25

respondents advising that they have plans to introduce such a service. This will take the total to 68% of respondents with such a service. Privacy culture and privacy protection legislation and policies were given as the main reasons for not having a central identity register.

- Of these, 4 of 11 respondents (Austria, Estonia, Japan and Spain) advised that the service satisfied all the identity authentication needs for all their tax administration electronic services, while a further three (Germany, South Africa and Belgium) advised that they had planned developments that would ensure their needs were fully satisfied in this area. Five of 11 respondents (Denmark, Finland, Norway, Portugal and Singapore) advised that the service did not satisfy all their needs.
- Belgium and Denmark provided information on the national services provided in their countries described in Box 1 and Box 2 below.

Table 2. National services provided by surveyed revenue bodies

Country	National identity register is run centrally	Revenue body supplements register with own data	National electronic identity authentication service is provided for tax administration	The national electronic identity authentication service satisfies the identity authentication needs for all e-services
Australia	✓*	✓	x	
Austria	✓	x	✓	✓
Belgium	✓	✓	✓	Planned
Canada	x		x	
Chile	✓	✓	x	
China	✓	✓	x	
Denmark	✓	✓	✓	x
Estonia	✓	Planned	✓	✓
Finland	✓	x	✓	x
France	✓	x	x	
Germany	x		✓	Planned
Ireland	x		x	
Italy	✓	✓	Planned	Planned
Japan	✓	x	✓	✓
Korea	✓	✓	x	
Mexico	✓	✓	Planned	Planned
New Zealand	✓		Planned	Planned
Norway	✓	✓	✓	x
Portugal	✓	✓	✓	x
Singapore	✓	✓	✓	x
South Africa	✓	✓	✓	Planned
Spain		✓	✓	✓
Sweden	✓	x	Planned	Planned
Turkey	✓	✓	Planned	Planned
USA	x		x	
Total (Yes)	20	13	12	4

* - for business

Box 1. How identity authentication is effected in Belgium

Belgium reported on the service operated across the public service administration in their jurisdiction. An authentication X509 certificate and corresponding private key is added to every citizen's electronic ID card (mandatory > 12 years). The private key can only be unlocked via a PIN code that is chosen by citizens when they receive their card. The card must be inserted into a Smartcard reader whose middleware must have been previously installed in the individual's PC. Part of the installed middleware includes an extension for popular browsers to allow the browser to communicate with the card. Authentication is initiated by the server, which requests an SSL two way connection to be opened between the browser and the server. For the client authentication, the browser requests the user to select among the available known certificates, including the one existing in the individual's electronic identity card. After the certificate's card selection, the individual is asked by the middleware to prove its identity by unlocking the card's private key with his/her PIN number. When successfully opened, the server uses the identity (national number) existing in the certificate to open a session for the individual.

Box 2. The electronic identity authentication service in Denmark

Denmark advised that the national electronic identity authentication service was designed by national standards that are guaranteed by an independent data protection agency operating within the Ministry of Justice. A licensed third party service provider operates the service. Individuals and businesses can obtain an electronic identity certificate via their bank, a tax office or via the Internet homepage of the third party service provider. As proof of identity, the individual must provide either his/her passport or (national, EU or EEA) driver's licence; or a police /military / NATO ID; or a permanent residency permit. An electronic certificate consists of a printed code card or a digital token or mobile phone plus a User ID and a password. This electronic ID cert is not installed on the PC, but can be used on any computer that has Java installed. Individuals can use the electronic ID to log into public services and Internet banking. The electronic ID for businesses can be used by employees, managers and business owners as personal ID on public and private homepages. The first person in a business signing up for the electronic ID is automatically made an administrator in the business and this person can then authorise other persons in the business to have the right to act on behalf of the business.

Private trusted third party identity authentication services

35. Many revenue bodies, when reviewing their business strategies, are asking themselves the questions "what is the primary purpose of my organisation?", and "what are my core competencies?" With a potential agenda of things they need or want to do which is greater than their available resources, they are asking themselves the follow-up question "does everything have to be done internally?" Identity authentication services do not necessarily need to be provided by a revenue body directly, and a number may have determined that others are better able to provide these services than they are themselves.

36. This area of the study sought to explore how tax administrations implement identity authentication provided by a trusted third party and the issues that this type of service raises. The survey posed the following questions (refer to Annex 2 for the detailed responses):

    1) Does your revenue body have a private trusted third party providing an identity authentication service? If yes, describe. What identity authentication and security issues have arisen?

    2) Are the identity proofs required the same as the identity proofs required for the national identity register? If no, describe the differences.

    3) What identity information is held by the trusted third party?

    4) Does the trusted third party identity register interface with your revenue body?

    5) What are the benefits to your revenue body from having a trusted third party identity authentication system?

    6) What are the benefits to your revenue body from having a trusted third party identity authentication system?

    7) If you do not use a private third party identity authentication service, why not?

37. The key findings from this aspect of the survey are set out hereunder:

- Sixteen of 25 (64%) respondents advised that they either use a national or third party identity authentication service and a further three respondents advised that they plan to introduce one, which will take the total to 76% (see Table 3).
- A significant 48% (12/25) indicated that they have a private trusted third party providing an identity authentication service. Twelve respondents noted that they do not have such a service, while the single remaining respondent (Italy) advised that one is planned.
- For those who do so, the use of private trusted third party to provide Identity Authentication service is reported to work well and no issues were reported that related specifically to the fact that a third party provided the Identity Authentication service.
- Survey respondents identified the following benefits to tax administrations (and other parties) from having a trusted third party identity authentication system: savings to the tax administrations in terms of financial and human resources and efficiencies; opportunities to reach a wider number of potential e-Service users; high level of satisfaction with the authentication method and level of performance of the third party; taxpayer convenience; savings for business and government; reduced taxpayer burden due to use of the same identity authentication as used in the private sector; and easy and secure access for parties involved.
- Other survey respondents identified data protection issues in providing taxpayer data to a third party, no requirement for a third party service and no third party service available as the main reasons why tax administrations have not engaged with private third parties to provide identity registers or identity authentication services.
- Of the 12 respondents that have a private trusted third party providing identity authentication, six (Austria, Denmark, Estonia, Finland, Japan and Sweden) reported that the identity proofs required were the same as the identity proofs required for the national identity register; New Zealand noted that they do not have a national register; Australia do not have a national identity register for individuals, but do for businesses; and of the remaining three respondents details of differences were noted in two cases (South Africa and Spain).
- Survey responses indicated that of the 12 respondents that have a private trusted third party providing identity authentication, in six cases (Austria, Denmark, Finland, Korea, Japan and Sweden) certain information is held by the third party. Sweden advised that the private trusted third party own the customer data and government agencies pay for access.
- Of the 12 respondents that use a trusted third party identity authentication service, only five (Australia, Denmark, Estonia, Korea and Norway) reported that the third party register interfaces with their tax administration.
- Across the 12 respondents that reported that they do not use a private third party identity authentication service a variety of reasons for this position were provided (see Annex 2, Question 6).

Table 3. The use of a private trusted third party identity register and/or authentication service

Country	The revenue body has a private trusted third party to provide an identity authentication service	The identity proofs required are the same as the identity proofs required for the national identity register	The private trusted third party identity register interfaces with your revenue body
Australia	✓	x	✓
Austria	✓	✓	X
Belgium	x		
Canada	x		
Chile	x		
China	x		
Denmark	✓	✓	✓
Estonia	✓	✓	✓
Finland	✓	✓	x
France	x		
Germany	x		
Ireland	x		
Italy	Planned	Planned	Planned
Japan	✓	✓	x
Korea	✓	x	✓
Mexico	x		
New Zealand	✓	Planned	x
Norway	✓	x	✓
Portugal	x		
Singapore	x		
South Africa	✓	x	x
Spain	✓	x	x
Sweden	✓	✓	x
Turkey	x		
USA	x		
Total (Yes)	12/25	6/12	5

Taxpayer and tax intermediary first registration with the revenue body

38. Registering for a service for the first time usually requires different and often more stringent proof of identity to that required for subsequent use of the service. This area of study examined the procedures in place to authenticate the identity of taxpayers and tax intermediaries who are registering with the tax administration for the first time. It also sought to identify how taxpayers are linked to their tax intermediary on the administrations records.

39. This section was examined under the following headings:

- Identity Authentication: Taxpayer's first registration with the revenue body
- Identity Authentication: Tax intermediary's first registration with the revenue body
- Linking of taxpayers with their tax intermediary on the revenue body's records.

40. The key findings in respect of these aspects are set out hereunder:

Identity authentication: taxpayer's first registration with the revenue body

- Twenty of 25 respondents advised that they use identity proof information from a national or private third party identity register for new taxpayer registrations, whilst only five respondents have neither a national nor a private third party identity register

providing the administration with the required taxpayer identity information to register a new taxpayer.

- A variety of identity proof information is required for the registration of **business corporate taxpayers.** The main types of identity information proofs advised were registration information from the Companies Office, including certificate of incorporation, and information on any Directors of the company, information from business regulatory authorities, face-to-face business visits.
- In many countries, corporate registration information from the Companies Office or equivalent including a certificate of incorporation and information on any Directors of the company must be provided. A few countries use identity information from a third party (e.g. Australia use the Australian Securities and Investment Commission and Singapore use the Accounting and Corporate Regulatory Authority). Other proofs reported included photo id and face-to-face meetings, and Ireland reported that a site visit is required, in certain circumstances, to validate a registration application if the company is registering for Value Added Tax (VAT).
- Similarly, a variety of identity proof information required for the registration of **business individual taxpayer**. The main types of identity information proofs advised were Business Number issued by the regulatory authorities, personal social insurance numbers, identity proofs from local registers of residents, date of birth or photo identification.
- Respondents reported a variety of identity proof information required for the registration of an individual business (non corporate). Australia requires a business applicant to provide an Australian Business Number issued by the Australian Business Register (administered by the ATO). Canada requires an individual business applicant to provide a Social Insurance Number from Service Canada.[4] Ireland advised that an applicant must provide a valid Personal Public Service Number (PPSN)[5] issued by the Department of Social Protection. A site visit might also be required to validate a registration if the business is registering for VAT. Singapore advised that an applicant will receive a Unique Entity Number (UEN) upon first registration with the Accounting and Corporate Regulatory Authority (ACRA), who maintains a national register for incorporated and non-incorporated businesses. The Inland Revenue Authority of Singapore will electronically obtain all relevant registration information, including the UEN, directly from the ACRA to include eligible businesses in the tax base, thereby removing the need for businesses to register separately with the tax authority. Other proofs requested by administrations include date of birth, photo identification. Germany advised that a business identity is verified with local registers of residents.
- In general, **employees** register with the revenue body using their social insurance number or equivalent or a national ID document.

  Some administrations advised that they offered a number of options to an employee seeking to register. For example New Zealand advised that there are a number of ways an employee can register. The applicant can provide an ID document from each of two categories, each including a photo ID. If this requirement cannot be met the person is asked to provide proof of identity from a third category. If again the applicant cannot satisfy that option the applicant is offered another category of identity proofs and the applicant is interviewed.

---

[4] Service Canada was created in 2005 to improve the delivery of government programs and services to Canadians, by making access to them faster, easier, and more convenient. The service offers single-window access to a wide range of Government of Canada programs and services for citizens. The Social Insurance Number was created in 1964 as a file identifier to be used for Canadian programs.

[5] Identity proofs required for an Irish PPSN are: For Irish citizens: 1. Birth Cert, 2. Valid photo ID; For UK citizens: 1. Passport/Birth cert, 2. Photo ID, 3. Evidence of address in Ireland; For EU/EEA citizens: 1. Passport/National ID 2. Evidence of address in Ireland; For Non-EEA citizens: 1. Passport or Certificate of Registration with Department of Justice, Equality & Law Reform (Immigration Card), 2. Evidence of address in Ireland.

Identity authentication: tax intermediary's first registration with revenue body

- All respondents with the exception of Finland advised that they facilitate tax intermediaries. Some administrations are quite flexible about the type of person that will be accepted as an authorised advisor. This can range from a family member to lawyers, tax practitioners and professionals with qualifications through a professional association; whereas other administrations advised that tax intermediaries are regulated and must have a recognised professional qualification and or be a member of a recognised professional association.
- To register a tax intermediary with the revenue body, nine countries advised that the tax intermediary must provide a national ID as proof of identity, whilst for seven proof of an agent's professional qualification through a professional association is required.
- Australia advised that both tax practitioners and what are known as business activity statement agents (BAS agents) can be authorised to provide intermediary services to a taxpayer. Denmark advised that 'personal advisors' for example family members, lawyers, accountants etc. can be authorised advisors by the taxpayer as well as a tax practitioner. The personal advisor must provide a number from the business register system or personal ID card in order to register with the Danish tax authority. The Canada Revenue Agency (CRA) advised that it operated a similar system to Denmark whereby family members, or other individuals, can be authorised to represent a taxpayer. In the case of e-filing a tax return on behalf of a taxpayer, the CRA will conduct a screening after which the 'e-file agent' will be provided with an e-filer number and password. New Zealand, Ireland and USA advised that they facilitate payroll agents.
- In Germany taxpayers may e-file tax declarations asking a third party to act as a "technical" data transmitter. When transmitting an electronic tax declaration, authentication of the data transmitter (not necessarily the tax payer) is requested. Any third party data transmitter has to inform the tax payer of data transmitted on his behalf. In case of error the tax payer has to correct the tax declaration. Data transmitters are liable for tax losses caused by unauthorised data transmissions. The special rights of tax consultants are not affected.

Linking of taxpayers with their tax intermediary on the revenue body's records

- Survey responses indicated that the majority of administrations require that a tax intermediary must hold evidence of a power of attorney or other formal declaration or mandate from their client instructing the Tax Intermediary to act on their behalf, and that most administrations hold an electronic record of the link between the taxpayer and intermediary. Six respondents advised that the client-intermediary link is stored on their tax database.
- Austria and the USA require a power of attorney from the client before the intermediary is permitted to represent a taxpayer. In Australia tax intermediaries are permitted to add clients using the appropriate Internet portal. Denmark advised that the taxpayer can create a link to an intermediary using an online system. Italy, Ireland and Chile require a formal declaration or mandate from the client is required. In Ireland an intermediary is provided with an application on the Revenue Online Service (ROS) to facilitate the delegation of a wide range of restricted client authorities to his or her office staff.
- Some respondents advised that an intermediary authority can be restricted to particular tax types for a client. Other respondents advised that the intermediary authority can be further defined e.g. Canada advised that the authority can be restricted to period level with a specific tax year and further restricted to view a record or amend a record.
- Korea advised that tax intermediaries are permitted to add or delete their taxpayer clients using hometax service (hometax service is a kind of internet portal for a taxpayer service delivery) and are also can be restricted to particular tax types for their taxpayer clients. If a tax intermediary is authorized only to fill tax a return for their taxpayer clients, they are restricted to the period of filing the tax return. Taxpayers are permitted to delete their tax intermediaries having a power of attorney but not permitted to add them. The link

between the taxpayer and tax intermediary is stored on the tax database of the National Tax Service.

Channels of identity authentication

41. As described in paragraph 16 (above), the study considered the seven main current and emerging channels for the access of electronic services, namely; the Internet; email (comprising both secure e-mail and standard e-mail); Telephony (comprising: voice; SMS/text services; interactive voice recognition services; and services accessed via intelligent mobile devices). In doing so we were able to identify the security and authentication methods in use, and issues faced, as well as gauge the overall maturity at this time of the service channel within a revenue body context through the capture of data on the extent of the use of each channel by each revenue body for the provision of services across the four customer groups (see paragraphs 66-67 as well as graphs 1-3).

Identity authentication: Internet services

42. This part of the study examined the methods used to authenticate the identity of taxpayers using tax services provided on the Internet, by examining the token(s)/system used to access the Internet service, the identity proofs required and the reason(s) for the option selected, across the four customer segments: corporate business, individual business, employee and tax intermediary.

43. The survey posed the following questions (refer Annex 3 for detailed revenue body responses):

    1) What systems or tokens do taxpayers use to access the Internet services?
    2) What identity proofs are required to register for Internet services?
    3) How do you assure identity authentication?
    4) Why did you choose this token/system and authentication proof for this service?
    5) What are the main issues identified with the identity authentication systems in use and were appropriate, what solutions to these issues have been implemented or planned?

44. The key findings are set out hereunder: (see Table 4)

- All 25 respondents indicated that they offer services on the internet channel, and across the countries a variety of systems/tokens are in place. The most common systems/tokens used are one or a combination of the following: Digital Certificate, User ID, PIN and Password. Other tokens used include Code Card, Electronic ID card, Shared Secrets/tax records and National ID. A number of respondents offer a Digital Certificate that can be used on a smartcard, mobile phone, security stick or soft PSE.[6]
- Many revenue bodies use different systems/tokens for different services. In general, this reflects the different authentication strengths required for different Internet services. For example, Japan requires a User ID number and Password for viewing tax account information, amending taxpayer basic information and viewing confidential information sent by the tax administration, but requires a digital certificate/digital signature in addition to user ID number and Password for filing a return, amending return details and claiming repayments.
- Denmark has introduced a digital certificate system where the citizen's private certificate is stored on a secure central server. Access to the certificate requires a username, a password and a challenge code from a code card. This particular method of storage of the digital certificate overcomes many of the hardware and storage problems that make digital certificates difficult for taxpayers to use.
- There are three common methods in use to protect against identity repudiation; 1) nine respondents advised that the use of digital certificates (PKI) assures against repudiation of

[6] A "Soft PSE" is a non-hardware based "Personal Security Environment"; most likely this is a digital certificate that can be stored either on a hard disk or a USB stick.

identity; 2) seven respondents use database logs and audit trails; 3) four respondents use the terms and conditions that a taxpayer has to accept in order to use the service.

- Survey responses indicated that across the countries that offer Internet services, a variety of identity proofs are required to register for Internet services, with most respondents reporting that they used one, or a combination of the following: personal/ national ID number, tax ID number, name, date of birth (DOB), birth certificate, data matching against tax administration's records, social security number, national business ID number, postal code, Digital Certificate, password, corporate data, information regarding the legal representative of a company.
- A number of respondents reported that their registration process used a separate channel as a security measure during the application process. In all cases, this involved out-of-band[7] step in the authentication process using land mail (Canada, Ireland, Norway, Germany) (Note: In relation to assuring identity authentication, Portugal and Ireland noted that the password required to use the service is sent to the taxpayer registered address held on the Tax Administration records.
- Sweden and Japan advised that the banking industry acts as a trusted third party in providing some secure online services on behalf of the tax administration e.g. filing tax payments through Internet banking. Mexico and USA are the only respondents who advised that they use biometrics as part of identity authentication.
- In terms of how identity authentication and non-repudiation is assured, countries use a number of methods in use to assure non-repudiation of identity. All respondents expressed satisfaction with the method in use in their own administration. Nine countries use digital certificates (PKI) to assure against repudiation of identity. Seven use database logs and audit trails as a measure to assure against repudiation of identity (five of these reported that access to the backend database(s) is strictly controlled). Four use the terms and conditions that a taxpayer has to accept in order to use the service to assure against repudiation of identity. Not all of the respondents that use the T&C use digital certificates e.g. France use a 'click and confirm' function on their website for customers who access the site using e-mail/password.
- Survey responses indicated that the two principal factors influencing administrations' choice of tokens/ systems and authentication proofs for this channel of communication are **strength of security** offered and **ease of use**. Other factors identified included: ease of implementation; ease of access by taxpayers and intermediaries; based on Industry standard; reliability; proven model; cost effective. Certain administrations (e.g. Norway, Sweden, Denmark and Australia) advised that their selection was influenced by government strategy and the fact that the service was operating within a common system for authentication across public services (and also the private sector i.e. in cases where the banking industry is involved). One country (Singapore) advised that their authentication system was able to leverage on government-wide identity registers and authentication services; while two other respondents (Germany and Ireland) indicated that compliance with legal requirements was an influencing factor.
- Fourteen of 25 respondents reported that they have had issues offering services over the Internet. Although a variety of issues were reported they can be categorised as relating to three main areas: digital certificates, identity authentication and end-user knowledge. These are detailed in Annex 3.

[7] Out-of-Band Authentication is the use of two or more separate communications channels communicate different parts of the registration process to the taxpayer e.g. Internet to apply for registration, password issued by land mail.

Box 3. Increasing uptake in the use of electronic services in France

After a year of no increase in the numbers using its secure electronic services, France experienced a 32% increase in the number of taxpayers electronically filing the income tax return in 2009. This increase was as a consequence of a number of innovations made to boost the number of e-filing, one of them (and probably the most visible) being the access through shared secrets.
Starting in 2012, the French administration intends to give up the electronic certificate totally and offer access to the administrations electronic services through a new 'whole-of-government portal' (mon.service-public.fr), in addition to the current shared secrets access to its electronic services. The new 'whole-of-government portal' will provide access authentication using e-mail and password.
France also advised that a new e-mail and password authentication was made available for business taxpayers in October 2010 (in addition to the electronic certificate authentication). After half a year in use, the number of businesses using the e-mail and password to authenticate is rapidly increasing, with an average to date of 44%. More than 90% of new business users chose the e-mail and password authentication system in preference to digital certificates. France advised that no specific issues had arisen so far with the new authentication service.

Table 4. Summary of Internet services provided by revenue bodies

Country	Services provided to the different customer groups (C- corporate business, I- individual business, E- employee taxpayer, T- tax intermediary)							
	View tax account information	File a return	Amend return details	Amend taxpayer basic information e.g. name & address	Make a payment/ submit payment instructions on a client's behalf	Claim repayments/ credits/ allowances	Submit bank account details	View confidential information sent by the tax administration
Australia	C,I,T	C,I,E,T	C (planned),I,T	C,I,T	C,I,E,T	C,I,E,T	C,I,E (planned),T	C,I,E (planned),T
Austria	C,I,E,T	C,I,E,T	C,I,E,T	C,I,E,T	C,I,E,T	C,I,E,T	-	-
Belgium	C,I,E,T	C,I,E,T	C,I,E,T	C,I,E,T	C,I,E,T	-	C,I,E,T	C,I,E,T
Canada	C,I,E,T	C,I,E,T	C,I,E,T	I, E	C,I,E	C,I,E	C, I, E	-
Chile	C,I,E,T	C,I,E,T	C,I,E,T	C, I, E	C,I,E	C, I, E	C, I, E	C, I, E
China	C, I	C, I, T	-	-	C,I	-	C, I	C, I
Denmark	C,I,E,T	C,I,E,T	C,I,E,T	-	C,I,E,T	C,I,E,T	-	C, I, E, T
Estonia	C,I,E,T	C,I,E,T	C,I,E,T	C,I,E,T	-	C,I,E,T	-	C, I, E, T
Finland	C,I,E(planned)	C,I,E	C,I,E	C,I,E	C,I	C	C,I,E	I(planned)
France	C,I,E,T	C,I,E,T	E (planned)	C,I,E,T	C,I,E,T	C,I,E (planned),T	-	-
Germany	C,I,E,T	C,I,E,T	-	-	-	-	-	-
Ireland	C,I,E,T	C,I,T	C,I,T	-	C,I,T	C,I,E,T	C,I,E	C,I,E,T
Italy	C,I,E,T	C,I,E,T	-	C,I,E,T	C,I,E,T	C,I,E,T	C,I,E,T	C,I,E,T
Japan	C,I,E	C,I,E,T	C,I,E,T	C,I,E	C,I,E,T	C,I,E,T	C,I,E,T	C,I,E
Korea	C,I,E,T	C,I,E,T	C,I,E,T	C,I,E,T	C,I,E,T	C,I,E,T	C,I,E,T	C,I,E,T
Mexico	C,I,E	C,I,E	C,I,E	C, I, E	-	-	-	-
New Zealand	C,I,E,T	C,I,E,T	C,I,E,T	C,I,E,T	C,I,E,T	T	C,I,E,T	C,I,E,T
Norway	E (planned)	C,I,E,T	C,I,E,T	C,I,E,T	C,I,E,T	-	C,I,E,T	C,I,E,T
Portugal	C,I,E,T	C,I,E,T	C,I,E,T	C,I,E	-	C,I,T	C,I,E,T	C,I,E
Singapore	C,I,E,T	C,I,E,T	C,I,E,T	E (planned)	C,I,E,T	C,I,E,T	-	C,I,E,T
South Africa	C,I,E,T	C,I,E,T	C,I,E,T	C,I,E,T	C,I,E,T	C,I,E,T	C,I,E,T	C,I,E,T
Spain	C,I,E,T	C,I,E,T	C,I,E,T	C,I,E,T	C,I,E,T	C,I,E,T	C,I,E,T	C,I,E,T
Sweden	C,I,E,T	C,I,E,T	C,I,E,T	C,I,E,T	C,I,E,T	-	C,I,E,T	C,I,E,T
Turkey	C,I,E,T	C,T	C,T	C,T	-	-	-	-
USA	I,E,T	C	C	-	C,I,E	-	I,E	-
Totals (P=planned)	C-23 I-24 E-21 & 2P T-20	C-25 I-23 E-21 T-22	C-20 & 1P I-19 E-17 & 1P T-18	C-17 I-18 E-16 & 1P T-13	C-20 I-20 E-17 T-15	C-16 I-15 E-13 & 1P T-14	C-16 I-17 E-15 & 1P T-11	C-17 I-17 & 1P E-15 & 1P T-13

Identity authentication: secure e-mail

45. This part of the study sought to explore the identity authentication methods used to authenticate the identity of taxpayers and tax intermediaries using tax services provided by secure e-mail.

46. The survey posed the following questions, the responses to which are set out in Annex 4:

    1) What systems or tokens do taxpayers use to access secure e-mail services and what identity proofs are required to register for secure e-mail services?

    2) Why did you choose this token/system and authentication proof for this service?

    3) How do you assure identity authentication and non-repudiation?

47. The key observations and findings are set out hereunder: (see Table 5)

- Seven of 25 revenue bodies indicated that they offer services on this channel, and for those that do, a variety of tokens/systems is in place. Most respondents advised that they used one, or a combination of the following: 1) digital certificate; 2) user ID, password; 3) registered e-mail address; 4) code-card challenge; and/or electronic ID.
- Most respondents advised that their administration used the same token/ system for all taxpayer types and for all services available on secure e-mail.
- In relation to Identity Proofs, a variety of identity proofs are required. Most respondents advised that they used one, or a combination of the following: 1) personal/ national ID number; 2) tax ID number; 3) electronic ID; 4) taxpayer contact information and personal details (e.g. name, date of birth); 5) data matching against tax administration's records; 6) social security number, national business ID number; and/or 7) digital certificate.
- Some administrations advised that they provide the equivalent of an e-mail service within their secure services system on the Internet i.e. messages can be interacted as a service within the administrations secure tax services on the Internet. This approach has many advantages over e-mail channels:
    - No separate e-mail channels required
    - Better security and identity authentication
    - Better information available about the taxpayer
    - Good opportunities to control messages and automate responses
    - Reduction in secure e-mail/standard e-mail administration costs
    - A good service to attract taxpayers to sign up to the Internet service.
    - According to survey responses the most common factors influencing administrations' choice of token/ system and authentication proofs for this channel were **ease of use** and **strength of security.** A number of respondents identified additional factors in this area as follows: Australia, Denmark and Sweden advised that their selection was influenced by government strategy and the fact that the system was operating within a common system for authentication across public services; Singapore noted that their system was able to leverage on government-wide identity registers and authentication services; respondents also identified factors such as ease of implementation, ease of accessing citizens and mobility (i.e. no hardware required).
- In terms of how identity authentication and non-repudiation is assured, Australia, Denmark and Singapore indicated that confidential information is returned to the taxpayer using their online portal/digital certificate. Ireland advised that the taxpayer must register for the secure e-mail service and accesses the secure e-mail using a system generated password that is issued to the taxpayer by land mail. New Zealand advised that they assure identity through a stringent registration system and a password.

Table 5. Summary of secure e-mail services provided by revenue bodies

Country	Services provided to the different customer groups (C- corporate business, I- individual business, E- employee taxpayer, T- Tax intermediary)							
	Request tax account information	File a return	Amend return details	Amend taxpayer basic information e.g. name & address	Make a payment/ submit payment instructions on a client's behalf	Claim repayments/ credits/ allowances	Submit bank account details	View confidential information sent by the tax administration
Australia	C, I, T	-	C, I, T	C, I, T	C, I, T	C, I, T	C, I, T	C, I, T
Austria	-	-	-	-	-	-	-	-
Belgium	-	-	-	-	-	-	-	-
Canada	-	-	-	-	-	-	-	-
Chile	-	-	-	-	-	-	-	-
China	-	-	-	-	-	-	-	-
Denmark	-	-	C, I, E, T	-	C,I,E,T	C,I,E,T	-	-
Estonia	C,I,E,T	C,I,E,T	C,I,E,T	C,I,E,T	-	C,I,E,T	-	C,I,E,T
Finland	-	-	-	-	-	-	-	-
France	-	-	-	-	-	-	-	-
Germany	-	-	-	-	-	-	-	-
Ireland	C,I,E,T	-	C,I,E,T	C,I,E,T	C,I,T	C,I,E,T	-	-
Italy	C,I,E,T	-	C,I,E,T	-	-	C,I,E,T	-	C, I, E, T (all planned)
Japan	-	-	-	-	-	-	-	-
Korea	-	-	-	-	-	-	-	-
Mexico	-	-	-	-	-	-	-	-
New Zealand	C,I,E,T	-	C,I,E,T	C,I,E,T	C,I,E,T	C,I,E,T	C, I, E, T	-
Norway	-	-	-	-	-	-	-	-
Portugal	-	-	-	-	-	-	-	-
Singapore	C,I,E,T	-	C,I,E,T	C,I,E,T	-	C,I,E,T	C,I,E,T	C,I,E,T
South Africa	-	-	-	-	-	-	-	-
Spain	-	-	-	-	-	-	-	-
Sweden	-	-	-	-	-	-	-	-
Turkey	-	-	-	-	-	-	-	-
USA	C,I,E,T (all planned)	C,I,E,T (all planned)	C,I,E,T (all planned)	C,I,E,T (all planned)	C,I,E,T (all planned)	C,I,E,T (all planned)	C,I,E,T (all planned)	C,I,E,T (all planned)
Totals (P=planned)	C-6 & 1P, I-6 & 1P, E-5 & 1P T-6 & 1P	C-1 & 1P I-1 & 1P E-1 & 1P T-1 & 1P	C-7 & 1P I-7 & 1P E-6 & 1P T-7 & 1P	C-5 & 1P I-5 & 1P E-4 & 1P T-5 & 1P	C-4 & 1P I-4 & 1P E-2 & 1P T-4 & 1P	C-7 & 1P I-7 & 1P E-6 & 1P T-7 & 1P	C-3 & 1P I-3 & 1P E-2 & 1P T-3 & 1P	C-3 & 2P I-3 & 2P E-2 & 2P T-3 & 2P

Identity authentication: standard e-mail

48. This part of the study explored the identity authentication methods used to authenticate the identity of taxpayers using tax services provided by standard e-mail. The survey posed the following questions (refer to Annex 5 for detailed responses):

    1) What systems or tokens do taxpayers use and what identity proofs are required to use Standard e-mail services?

    2) How do you assure identity authentication?

    3) What issues have you identified and what solutions have you planned or implemented?

49. The key observations and findings are as follows: (see Table 6.)

    - Only 6/25 respondents indicated that they offer services using standard e-mail, and for those that do this is normally only used to communicate information that is not sensitive or confidential.
    - For those that do use this channel, **ease of use** and **ease of implementation** were identified as the main benefits, whereas poor data security and poor data confidentiality were identified as the main problems.
    - Most revenue bodies will accept e-mails containing sensitive or confidential information. However, administrations will normally reply using an alternative secure communications channel e.g. Secure e-mail, secure store within the administrations secure services portal, telephone, postal service. However, for some, sensitive or confidential information may only be delivered through this channel under particular circumstances which normally means by special arrangement with the taxpayer and where additional security arrangements are put in place.
    - The identity authentication methods, or tokens, required of taxpayers and tax intermediaries using this channel mostly involve the use of one or a combination of ID, reference numbers and personal details. In each case the method used to authenticate identity is by data matching against backend databases. Belgium advised that a business individual must include a reference number and a unique company code that is issued by land mail. An Employee must include their reference number that is comprised of their National ID number and another unique reference number.

Table 6. Summary of standard e-mail services provided by revenue bodies

Country	Services provided to the different customer groups (C- corporate business, I- individual business, E- employee taxpayer, T- Tax intermediary)							
	Request tax account information	File a return	Amend return details	Amend taxpayer basic information e.g. name & address	Make a payment/ submit payment instructions on a client's behalf	Claim repayments/ credits/ allowances	Submit bank account details	View confidential information sent by the tax administration
Australia	-	-	-	-	-	-	-	-
Austria	-	-	-	-	-	-	-	-
Belgium	-	-	-	-	-	-	-	-
Canada	-	-	-	-	-	-	-	-
Chile	-	-	-	-	-	-	-	-
China	-	-	-	-	-	-	-	-
Denmark	-	-	-	-	-	-	-	-
Estonia	-	-	-	-	-	-	-	-
Finland	-	-	-	-	-	-	-	-
France	C,I,E,T	-	E	E	-	-	-	-
Germany	C,I,E,T	-	C,I,E,T	-	-	-	-	-
Ireland	C,I,E,T	T	C,I,E,T	C,I,E,T	C,I,E,T	C,I,E,T	-	-
Italy	C,I,E,T	-	-	-	-	C,I,E,T	-	-
Japan	-	-	-	-	-	-	-	-
Korea	-	-	-	-	-	-	-	-
Mexico	-	-	-	-	-	-	-	-
New Zealand	-	-	-	-	-	-	-	-
Norway	-	-	-	-	-	-	-	-
Portugal	-	-	-	-	-	-	-	-
Singapore	-	-	C,I,E,T	-	-	C,I,E,T	-	-
South Africa	C,I,E,T	-	-	-	-	-	-	-
Spain	-	-	-	-	-	-	-	-
Sweden	-	-	-	-	-	-	-	-
Turkey	-	-	-	-	-	-	-	-
USA	-	-	-	-	-	-	-	-
Totals (P=planned)	C-5 I-6 E-6 T-5	C-0 I-0 E-0 T-1	C-3 I-3 E-4 T-3	C-1 I-1 E-2 T-1	C-1 I-1 E-1 T-1	C-4 I-4 E-4 T-4	C-0 I-0 E-0 T-0	C-0 I-0 E-0 T-0

Identity authentication: telephone (voice)

50. This part of the study considered the Identity Authentication methods used to authenticate the identity of taxpayers and tax intermediaries using tax services provided by telephone (voice). The survey posed the following questions (refer to Annex 6 for detailed responses):

    1) What systems or tokens do taxpayers use, why was this system or token selected and what identity proofs are required to use the telephone (voice) channel services?

    2) How do you assure non-repudiation?

    3) What issues have you identified and what solutions have you planned or implemented?

51. The key observations and findings are as follows: (see Table 7)

    - Fifteen of 25 administrations advised that they used the telephone (voice) channel to conduct interactive tax business.

    - Respondents indicated that across the administrations that offer services through telephone (voice), the token or system generally used is a verbal challenge validation process involving security question(s) to ensure the identity of the caller (e.g. tax reference number, social security number etc), and this verbal challenge is also the method to assure against a taxpayer repudiating a telephone (voice) transaction.

52. In relation to identity proofs, respondents noted a variety of proofs are used, with most reporting that they used a combination of the following: personal or company information, challenges using known information from tax records, national ID card, PIN, shared secret. Germany and Ireland reported that they use telephone recall as an additional security measure.

53. Most respondents indicated that in the case of doubt about the identity of the caller they provide the requested information through the postal system to the taxpayer's or tax intermediaries registered address.

54. The most common reported factors influencing administrations' choice of identity authentication methods for the telephone (voice) were; to uphold the integrity of the tax system, to ensure that taxpayer confidential or sensitive data remains confidential, relatively easy to use and less expensive and quicker to administer than the personal caller or postal correspondence services.

55. To assure identity authentication and non-repudiation, most countries rely on the strength of the verbal challenges policies in place in their administration. A few additional safeguards by individual countries were reported: The USA advised that any changes made, as a result of telephone (voice) instructions, are notified to the registered taxpayer by land mail at the address on file. Australia, New Zealand and Ireland advised that they record telephone (voice) calls. Canada advised that they rely on the strength of the registration process and integrity of other areas with the Canada Revenue Agency. Ireland and the USA reported that a call is terminated if any doubt arises as to the identity of the caller.

56. The only issue reported with the limited use of this channel was by New Zealand, who reported that people can become familiar with the process used to authenticate and possibly get the information required to answer the control questions correctly. New Zealand is considering the use of Voice Recognition Software as a way of counteracting this problem.

Table 7. Summary of telephone (voice) services provided by revenue bodies

Country	Services provided to the different customer groups (C- corporate business, I- individual business, E- employee taxpayer, T- Tax intermediary)							
	Request tax account information	File a return	Amend return details	Amend taxpayer basic information e.g. name & address	Make a payment/ submit payment instructions on a client's behalf	Claim repayments/ credits/ allowances	Submit bank account details	View confidential information sent by the tax administration
Australia	C, I, E, T	-	-	C, I, E	T	-	C, I, E, T	C, I, T
Austria	C, I, E, T	-	-	-	-	-	-	-
Belgium	C, I, E, T	-	-	-	-	-	-	-
Canada	C, I, E, T	-	C, I, E, T	C, I, E	T	C, I, E, T	E, T	-
Chile	-	-	-	-	-	-	-	-
China	-	-	-	-	-	-	-	-
Denmark	C,I,E,T	-	-	-	-	-	-	-
Estonia	-	-	-	-	-	-	-	-
Finland	-	-	-	I	-	-	-	-
France	C,I,E,T	-	-	E	-	-	-	-
Germany	C,I,E,T	-	C,I,E,T	-	-	-	-	-
Ireland	C,I,E,T	-	C,I,E,T	-	-	C,I,E,T	-	-
Italy	C,I,E,T	-	C,I,E,T	-	-	-	-	C,I,E,T
Japan	-	-	-	-	-	-	-	-
Korea	-	-	-	-	-	-	-	-
Mexico	-	-	-	-	-	-	-	-
New Zealand	C,I,E,T	-	C,I,E,T	C,I,E,T	E,T	C,I,E,T	E, T	C,I,E,T
Norway	-	-	-	-	-	-	-	-
Portugal	-	-	-	-	-	-	-	-
Singapore	C,I,E,T	-	I,E,T	-	-	I,E,T	-	-
South Africa	C,I,E,T	-	-	C,I,E,T	-	-	-	C,I,E,T
Spain	C,I,E,T	C,I,E,T	C,I,E,T	C,I,E,T	-	-	-	-
Sweden	-	-	-	-	-	-	-	-
Turkey	C,I,E,T (all planned)	C,I,E,T (all planned)	-	-	C,I,E,T (all planned)	C,I,E,T (all planned)	-	-
USA	C,I,E,T	-	-	C,I,E,T	C,I,E,T	-	C,I,E,T	-
Totals (P=planned)	C-14 & 1P I-14 & 1P E-14 & 1P T-14 & 1P	C-1 & 1P I-1 & 1P E-1 & 1P T-1 & 1P	C-6 I-7 E-7 T-7	C-6 I-7 E-7 T-3	C-1P I-1P E-2 & 1P T-4 & 1P	C-3 & 1P I-4 & 1P E-4 & 1P T-4 & 1P	C-2 I-2 E-4 T-4	C-4 I-4 E-3 T-4

Table 8. Summary of telephone (SMS) services provided by revenue bodies

Country	Services provided to the different customer groups (C- corporate business, I- individual business, E- employee taxpayer, T- Tax intermediary)							
	Request tax account information	File a return	Amend return details	Amend taxpayer basic information e.g. name & address	Make a payment/ submit payment instructions on a client's behalf	Claim repayments/ credits/ allowances	Submit bank account details	View confidential information sent by the tax administration
Australia	-	-	-	-	-	-	-	-
Austria	-	-	-	-	-	-	-	-
Belgium	-	-	-	-	-	-	-	-
Canada	-	-	-	-	-	-	-	-
Chile	-	C, I, E	-	-	-	-	-	-
China	-	-	-	-	-	-	-	-
Denmark	-	-	-	-	-	-	-	-
Estonia	-	-	-	-	-	-	-	-
Finland	-	-	-	-	-	-	-	-
France	-	-	-	-	-	-	-	-
Germany	-	-	-	-	-	-	-	-
Ireland	E	-	-	E	-	E	-	-
Italy	-	-	-	-	-	-	-	-
Japan	-	-	-	-	-	-	-	-
Korea	-	-	-	-	-	-	-	-
Mexico	-	-	-	-	-	-	-	-
New Zealand	-	-	-	-	-	-	-	-
Norway	-	-	-	-	-	-	-	-
Portugal	-	-	-	-	-	-	-	-
Singapore	-	-	-	-	-	-	-	-
South Africa	-	-	-	-	-	-	-	-
Spain	C,I,E,T	C,I,E,T	-	-	-	-	-	-
Sweden	-	E	-	-	-	-	C	-
Turkey	C,I,E	-	-	-	-	-	-	-
USA	-	-	-	-	-	-	-	-
Totals (P=planned)	C-2 I-2 E-3 T-1	C-2 I-2 E-3 T-1	C-0 I-0 E-0 T-0	C-0 I-0 E-1 T-0	C-0 I-0 E-0 T-0	C-0 I-0 E-1 T-0	C-1 I-0 E-0 T-0	C-0 I-0 E-0 T-0

Identity authentication: telephone– Short Message Service (SMS)

57. This part of the study sought to explore the Identity Authentication methods used to authenticate the identity of taxpayers and tax intermediaries using tax services provided by telephone (SMS). The survey posed the following questions (refer to Annex 7 for detailed responses).

    1) What systems or tokens do taxpayers use, why was this system or token selected and what identity proofs are required to use the telephone (SMS) channel services?

    2) How do you assure identity authentication and non-repudiation?

    3) What issues have you identified and what solutions have you planned or implemented?

58. The key observations and findings are as follows: (see Table 8)

    - Five of 25 respondents advised that they provide services using telephone (SMS). However, two of those respondents advised that they use telephone (SMS) to provide reminders and alerts only. The responses indicated that the extent of services available by telephone (SMS) is quite limited. Across the administrations that reported on their authentication systems for telephone (SMS), respondents noted a variety of tokens/ systems including: password, Digital Certificate, PIN, personal/National ID, and identity proofs including one or a combination of the following: ID number, Fiscal ID number, administration records, name, date of birth, address and contact details. Turkey advised that motor-vehicle license information is used for authentication.
    - Respondents indicated that confidential information is not generally sent to the taxpayer by telephone (SMS). Instead, when such information is requested by telephone (SMS) the requested information is sent to the taxpayer by an alternative channel of communication (e.g. postal system).
    - The most common factors that influence the choice of authentication methods for telephone (SMS) were ease of use and implementation and strength of security.
    - Limited information on the assurance of identity authentication and non-repudiation was provided by this channel, however, Chile advised that business corporate, business individuals and employees can file a return using telephone (SMS). Identity is authenticated through control questions that must be completed by the taxpayer, and Ireland authenticates identity by the taxpayer entering the secure PIN number issued by the administration. Ireland also advised that it retains a copy of the telephone number used to send the SMS. These two items are also used to protect against the taxpayer repudiating the transaction.

Identity authentication: telephone – Interactive Voice Response (IVR)

59. This part of the study examined the Identity Authentication methods used to authenticate the identity of taxpayers and tax intermediaries using tax services provided by telephone (IVR). The survey posed the following questions (refer Annex 8 for detailed responses):

    1) What systems or tokens do taxpayers use, why was this system or token selected and what identity proofs are required to use the telephone (IVR) channel services?

    2) How do you assure identity authentication and non-repudiation?

    3) What issues have you identified and what solutions have you planned or implemented?

60. The key observations and findings are as follows: (see Table 9)

    - Eleven of 25 respondents advised that they provide services using telephone (IVR)
    - Respondents advised that a variety of tokens/systems were in place, with most advising that they used a combination of various ID/ reference numbers and codes, password, PIN, personal data, revenue records, ID proofing, shared secrets and Digital Certificate.
    - Respondents advised that in general a variety of identity proofs are required, including the following: social insurance number, personalised access code, confirmation of identity information, national/ personal ID number, challenge for confirmation of

certain tax records data held by the administration, personal data, postcode, tax number, personal public service number, PIN, identifier of tax intermediary, national business ID number, tax records, document ID number issued by the administration, Digital Certificate, electronic national ID card, employer ID number. One country (USA) noted that a bank routing number is required to access the service 'Make a payment' (along with other identity proofs).

- Some respondents advised that secure information requested using this channel is not issued via this channel or that any credit claims etc entered through this channel are manually screened before processing. **This indicates that the channel is not regarded as a fully secure channel for conducting interactive secure services.**
- Additional security measures are in place where the risk is higher, e.g. where confidential information can be accessed (New Zealand, Singapore), or where a new PIN is requested (Ireland). Where confidential information is requested, it is generally sent to the customer via an alternative channel, i.e. post or the online portal.
- New Zealand has just (September 2011) launched Voice ID (Voice Biometrics capability) and have registered over a 1,200 customers in the last two weeks. They have higher than expected success rates with 98% successful registrations compared with approximately 75% for MSD or NAB, ensuring greater access to telephony IVR and surety of identity 24/7.
- The most common factors influencing revenue bodies' choice of authentication methods for IVR are **ease of use** and **security measures**. Additional factors noted were cost effectiveness (Canada) and to facilitate access to basic services (Spain).

Identity authentication: intelligent mobile devices

61. This part of the study sought to explore the identity authentication methods used to authenticate the identity of taxpayers and tax intermediaries using secure tax services provided by intelligent mobile devices. The survey posed the following questions:

    1) What systems or tokens do taxpayers use, why was this system or token selected and what identity proofs are required to use the Intelligent Mobile Device services?

    2) How do you assure identity authentication and non-repudiation?

    3) What issues have you identified and what solutions have you planned or implemented?

62. The key observations and findings were as follows: (see Table 10)

    - Three of 25 respondents advised that they provide services using Intelligent Mobile Devices. The range of services offered by these administrations is very limited.
    - Ireland offers employees the service 'Claim repayments, credits, allowances' via this channel of communication. The taxpayer's Personal Public Service Number (PPSN), a PIN and a secret question are required to submit a claim or claim a relief from a mobile application. This authentication method was chosen for ease of use.
    - USA offers business individuals and employees the service 'View/ request tax account information'. This allows very low risk data to be returned to the taxpayer, e.g. View the date of a refund to the taxpayer. This is a self Authentication Application using shared secret to validate identity.
    - Japan provides the mobile device's web browser function to make payments via internet banking.
    - New Zealand is currently prototyping a solution for mobile web services that will allow access to Customer specific tax and social policy information through a cut down version of their Online Services using existing authentication processes. When they put in place iGovt in 2012 (cross-government authentication process) this will sit across this emerging mobile channel.
    - There were no issues reported, however, Australia advised that…… "*The ATO does not currently offer services to mobile devices. Current prototyping of solutions*

for future electronic services includes provisional support for various mobile devices, however, not all mobile OS will be supported, at least in the initial releases."

Table 9. Summary of telephone services (including interactive voice responses) provided by revenue bodies

Country	Services provided to the different customer groups (C- corporate business, I- individual business, E- employee taxpayer, T- Tax intermediary)							
	Request tax account information	File a return	Amend return details	Amend taxpayer basic information e.g. name & address	Make a payment/ submit payment instructions on a client's behalf	Claim repayments/ credits/ allowances	Submit bank account details	View confidential information sent by the tax administration
Australia	C, I, E, T	C, I, E	-	-	C, I, E	I, E	C, I, E all planned	-
Austria	-	-	-	-	-	-	-	-
Belgium	-	-	-	-	-	-	-	-
Canada	-	E	-	-	-	-	-	-
Chile	-	C, I	-	-	-	-	-	-
China	I	I	-	-	I	-	-	-
Denmark	I,E	E	E	-	-	-	-	-
Estonia	-	-	-	-	-	-	-	-
Finland	-	-	-	-	-	-	-	-
France	-	-	-	-	-	-	-	-
Germany	-	-	-	-	-	-	-	-
Ireland	C,E,T	-	-	E, T	-	E, T	-	-
Italy	C,I,E,T	-	C,I,E,T	-	-	-	-	C,I,E,T
Japan	-	-	-	-	-	-	-	-
Korea	-	-	-	-	-	-	-	-
Mexico	-	-	-	-	-	-	-	-
New Zealand	C,I,E,T	E	-	I,E,T	-	-	-	-
Norway	-	-	-	-	-	-	-	-
Portugal	-	-	-	-	-	-	-	-
Singapore	-	-	-	-	-	-	-	-
South Africa	-	-	-	-	-	-	-	-
Spain	C,I,E,T	C,I,E,T	C,I,E,T	C,I,E,T	-	-	-	-
Sweden	-	E	-	-	-	-	-	-
Turkey	C,I,E,T (all planned)	C,I,E,T (all planned)	-	-	C,I,E,T (all planned)	C,I,E,T (all planned)	-	-
USA	I	-	-	-	I	-	I	-
Totals (P=planned)	C-5 & 1P I-7 & 1P E-6 & 1P T-5 & 1P	C-3 & 1P I-4 & 1P E-6 & 1P T-1 & 1P	C-2 I-2 E-3 T-2	C-1 I-2 E-3 T-3	C-1 & 1P I-3 & 1P E-1 & 1P T-1P	C-1P I-1 & 1P E-2 & 1P T-1 & 1P	C-1P I-1 & 1P E-1P T-1P	C-1 I-1 E-1 T-1

Table 10. Summary of intelligent mobile device services provided by revenue bodies

Country	Services provided to the different customer groups (C- corporate business, I- individual business, E- employee taxpayer, T- Tax intermediary)							
	View tax account information	File a return	Amend return details	Amend taxpayer basic information e.g. name & address	Make a payment/ submit payment instructions on a client's behalf	Claim repayments/ credits/ allowances	Submit bank account details	View confidential information sent by the tax administration
Australia	-	-	-	-	-	-	-	-
Austria	-	-	-	-	-	-	-	-
Belgium	-	-	-	-	-	-	-	-
Canada	-	-	-	-	-	-	-	-
Chile	-	-	-	-	-	-	-	-
China	-	-	-	-	-	-	-	-
Denmark	-	-	-	-	-	-	-	-
Estonia	-	-	-	-	-	-	-	-
Finland	-	-	-	-	-	-	-	-
France	-	-	-	-	-	-	-	-
Germany	-	-	-	-	-	-	-	-
Ireland	-	-	-	-	-	E	-	-
Italy	C, I, E, T (all P)	C, I, E, T (all P)	C, I, E, T (all P)	C, I, E, T (all P)	C, I, E, T (all P)	C, I, E, T (all P)	C, I, E, T (all P)	C, I, E, T (all P)
Japan	-	-	-	-	C, I, E	-	-	-
Korea	-	-	-	-	-	-	-	-
Mexico	-	-	-	-	-	-	-	-
New Zealand	-	-	-	-	-	-	-	-
Norway	-	-	-	-	-	-	-	-
Portugal	-	-	-	-	-	-	-	-
Singapore	-	-	-	-	-	-	-	-
South Africa	-	-	-	-	-	-	-	-
Spain	-	-	-	-	-	-	-	-
Sweden	-	E	-	-	-	-	-	-
Turkey	C,I,E,(all P)	-	-	C,I,E (all P)	-	-	-	-
USA	I,E	-	-	-	-	-	-	-
Totals (P=planned)	C-2P I-1 & 2P E-1 & 2P T-1 & 2P	C-1P I-1P E-1 & 1P T-1P	C-1P I-1P E-1P T-1P	C-2P I-2P E-2P T-2P	C-1 & 1P I-1 & 1P E-1 & 1P T-1P	C-1P I-1P E-1 & 1P T-1P	C-1P I-1P E-1P T-1P	C-1P I-1P E-1P T-1P

Summary of identity authentication across channels

Existing services

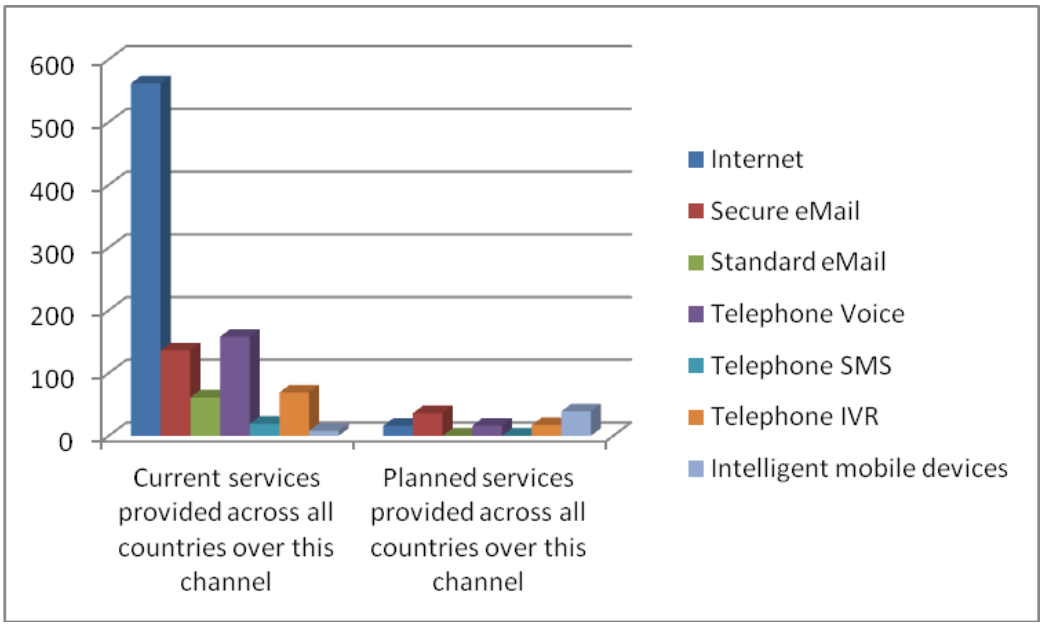
63. Across the 25 countries who participated in this study, the Internet is currently by far the most significant channel for conducting secure exchanges with customers. With four customer types examined (business corporate, business individual, employee and tax intermediary, and eight possible confidential services (view tax account information; file a return; amend return details; amend taxpayer basic information; claim a repayment / credit / allowance; submit bank account details; view confidential information sent by the tax administration), there were a total of 800 possible service events (four customer types * eight confidential interactions * 25 countries). Of these 562/800 are currently provided using the Internet. The next most significant although much less than the Internet, is Telephone (voice) with 158/800, followed by secure e-mail at 136/800. Telephone (IVR) at 69/800 and standard e-mail at 61/800 are used relatively little overall, whilst the use of telephone (SMS) (19/800) and intelligent mobile devices (8/800) are still very embryonic. See Graph 1 below.

Planned services

64. The picture is quite different when you look at planned services to be implemented, although the significance of these at this stage is still quite modest. The most significant channel for planned services is for intelligent mobile devices, where an additional 39/800 service events are planned, closely followed by secure e-mail with 36/800. Telephone IVR, telephone voice and the Internet, are all quite similar at 20/800, 16/800 and 12/800 respectively and there are no planned new service interactions in either standard e-mail or SMS in any of the countries. If these planned new service interactions are all implemented over the course of the next two years, they will have a relatively modest impact overall on the significance of the various channels in the strategies of the participant revenue bodies with two exceptions: secure e-mail will become as significant as telephone (voice) as the tie second most important channel; and the use of telephone (SMS) will fall below intelligent mobile devices into the position of least significant channel. See Graph 1 below.

65. However, as a word of caution, the world can change quickly in the age of digital services, and revenue bodies should continue to monitor both customer demand and channel maturity in other sectors, as this situation could change quite markedly even over the short and definitely over the medium term.

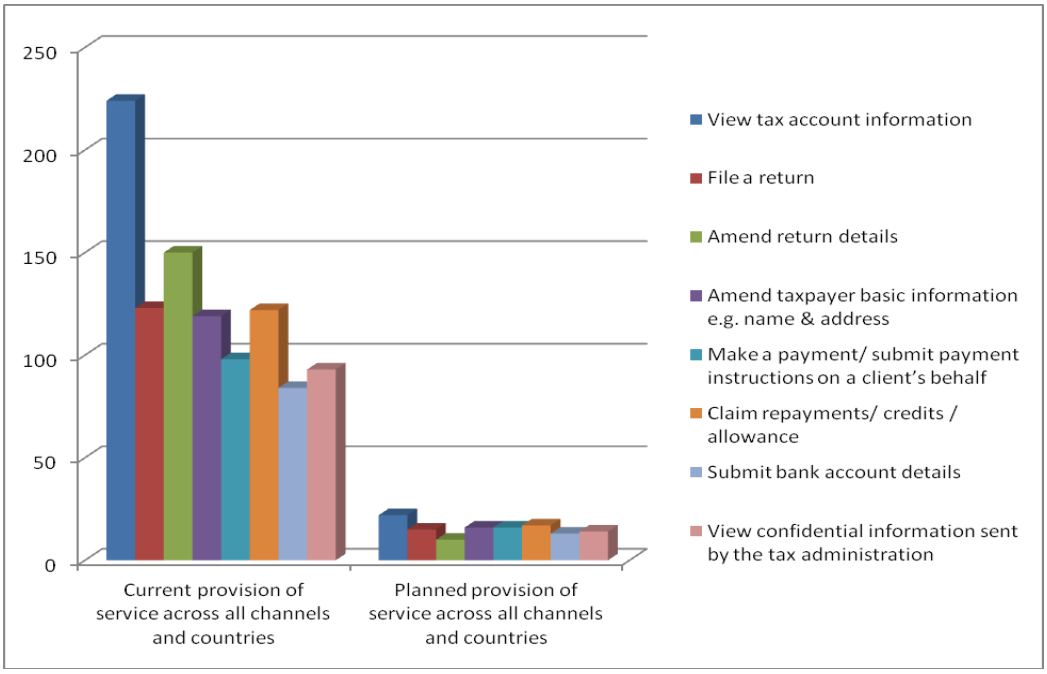
Graph 1. Total current and planned service interactions in each channel



Note: The maximum possible is 800 (eight services across four customer groups and 25 countries).

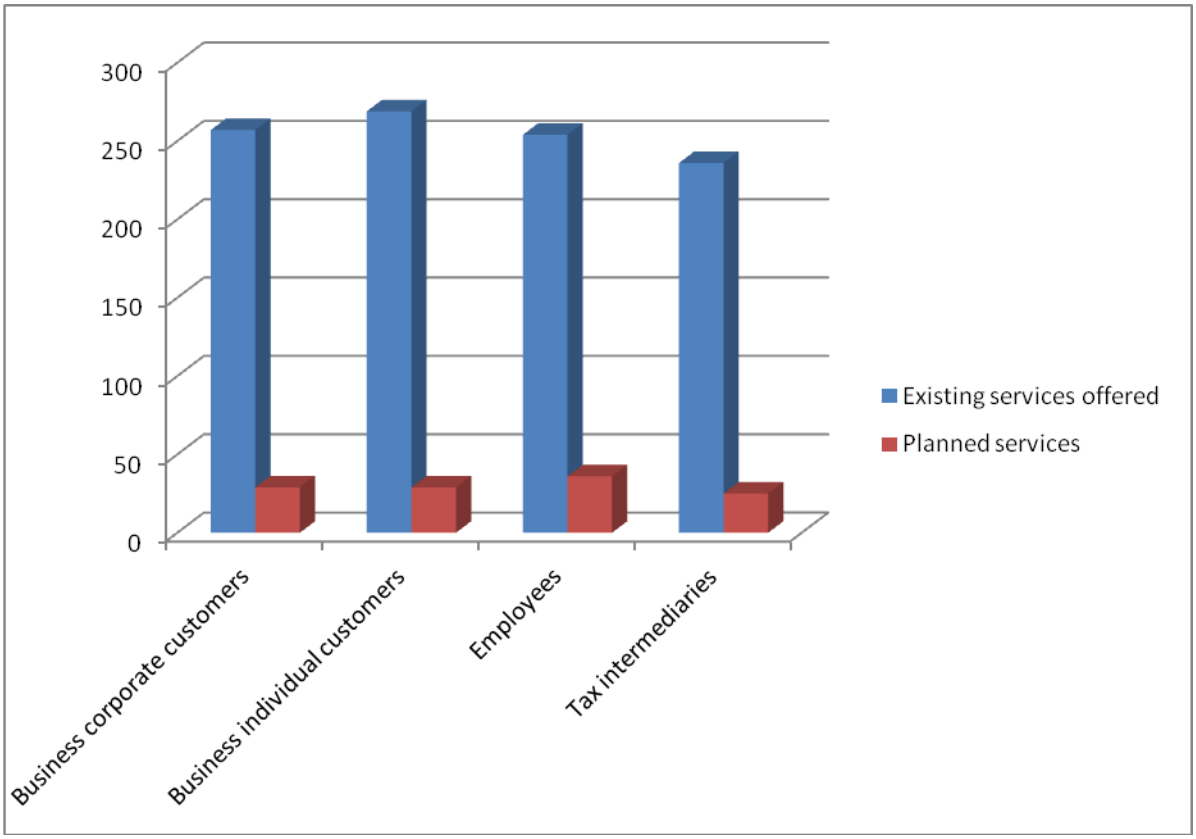
66. In terms of the most frequently provided service (across all customer groups and all countries), the ability to view tax account information is the most widely provided, at 224 times across the four customer groups and 25 countries, followed by amend return details at 150, and claim repayments / credits / allowances 122, file a return at 123, amend taxpayer basic information at 119, make a payment / submit payment instructions on behalf of a client at 98, view confidential information sent by tax authorities at 93, and submit bank account details at 84. None of the new planned services will have any impact on the relative positions of the services being provided. See Graph 2.

Graph 2. Frequency of specific services offered across all channels, customer groups and countries



67. Comparing the frequency of services offered to the four customer groups, there is minimal overall variation with 269 service interactions offered (out of a potential 1,344 if all eight services were offered across all seven channels in all 25 countries) to business individual customers with another 29 planned; 257 to business corporate customers, with another 29 planned; 254 to employees, with another 36 planned; and 236 to tax intermediaries, with another 25 planned. See Graph 3. Whilst outside the scope of this study, it is without doubt that there will be a significantly wider variation in revenue body key performance indicators against those customer segments. As it is a strategic priority for all revenue bodies to ensure they are getting a maximum return for their investments (vis-a-vis the current FTA study "Working Smarter in Service Delivery"), and on the general assumption that services offered broadly equate to investment required and resources consumed, revenue bodies might wish to assess whether they are directing such investments in the areas and to the customer groups where they will have the most impact.

Graph 3. Comparison of the number of services offered to different customer groups across all service channels and by all countries



IV. SECURING DATA/DOCUMENTS EXCHANGES

68. The information provided in Chapter III showed how revenue bodies confirmed the authentication of their taxpayers (that is, how they validated that they were indeed the individuals or organisations which they purported to be (the "who am I", and "how can I prove it" described in Box 1 below) and how they controlled access to a standard range of services which would typically be offered (the "what can I do" also described in the box).

69. This section of the study examines the methods and solutions adopted (or planned) by tax administrations to secure data and documents electronically exchanged between tax administrations and their taxpayers –i.e. ensuring confidentiality (how is the confidentiality of the data exchange assured), integrity (how do we assure that the data is complete, un-changed and un-corrupted) and non-repudiation (how do we assure that the source can be proven and that the exchange cannot subsequently be denied). As in Chapter III, the communications channels examined were: 1) Internet services; 2) secure e-mail services; 3) standard e-mail services; 4) telephony voice services; 5) telephony SMS/text services; 6) telephony IVR Services; and 7) intelligent mobile devices services.

70. The survey posed the following questions for each channel:

    1) How do you assure data exchange confidentiality?
    2) How do you assure data integrity?
    3) How do you assure non-repudiation?
    4) Are you satisfied with the overall strength of your solution?
    5) What Issues have you identified and what solutions have you planned or implemented?

Summary findings on securing data and document exchange

Internet, secure e-mail, standard e-mail, and intelligent mobile devices

- All 25 respondents offer services on the internet. Seven of 25 respondents offer services using the secure e-mail channel. Six of 25 respondents offer services using the standard e-mail channel, whereas only 4/25 respondents offer any service using Intelligent Mobile Devices.
- Data confidentiality using internet services is assured mainly by using Secure Socket Layer (SSL)[8] or similar encryption protocols e.g. digital certificates and hash algorithms. These systems are very easy to implement on the internet and provide good security.
- SSL or similar encryption protocols are used to assure confidentiality for secure e-mail. However, taxpayers have to register for this service type and must use an access token to access the service. This reduces the attractiveness of the service to taxpayers.
- Data integrity is mainly assured by hashing the data.[9] The majority of respondents indicated hashing to be of at least adequate strength. Digital Signatures using Public Key Infrastructure (PKI) can also be used to provide data integrity checks.[10]
- There is more variety in responses in relation to assuring data non-repudiation. Replies included the use of digital certificates, database logs, terms and conditions or shared

[8] SSL is at the "transport" level – the message is encrypted for confidentiality between the sender and receiver.

[9] A hash function is used to encrypt data by applying an algorithm with some seed values to scramble the data, which also allows the data to be later, decrypted with a certainty that the data has not been changed in anyway. This function can also be used to encrypt data for confidentiality.

[10] PKI - Public Key Infrastructure - basically this is a security protocol that uses a pair of 'keys', one *normally* [not always the case] held by the taxpayer and the other by the administration. A taxpayer uses their key to log in, sign and submit information which is compared against the key held by the administration. Both must match in order for data to be accepted or for the user to access information. Data is encrypted and decrypted. Commonly a password will also be used therefore the system has both a knowledge, technical and possession basis.

secrets. The overall strength of these methods is considered by respondents to be at least adequate.

- Standard e-mail is a very common and very easy system to use. The lack of any easy to use security services available on standard e-mail was the main issue identified for this channel, limiting the potential application of standard e-mail for interactions between a revenue body and its' taxpayers. Replies to the survey indicated that standard e-mail is not used by administrations to transact confidential data. Taxpayers are generally advised or precluded by administrations not to use standard e-mail for transacting confidential data with the administration, and are encouraged to use secure e-mail services or the internet where available. In nearly all circumstances reported, replies to confidential queries received by standard e-mail are responded to by land mail or through the administrations internet secure portal.
- Only two countries provided information on assurance for data exchange for intelligent mobile devices reflecting the very limited use of this channel at this stage (see below).

Telephone (Voice, IVR, and SMS)

- Fifteen of 25 respondents offer a secure information service using telephone voice. Eleven of 25 offer secure services using telephone IVR, but this is reduced to 4/25 for those offering secure service using telephone SMS.
- Data confidentiality, integrity and non-repudiation through the telephone service channels are generally assured by matching customer data, such as ID or customer number, with the records held by the tax administration. Where possible, i.e. for the IVR and SMS channels, SSL encryption or data hashing is used in combination with ID and password. The overall strength of these methods is indicated as strong or at least adequate for all telephone channels.
- Most respondents advised that they will conduct an identity proof assessment before conducting a confidential conversation by telephone. All respondents advised that they would terminate a conversation if there was any doubt about the identity of the caller. The communication would then be carried out mainly by land mail using the contact details stored on the administrations records.
- Most respondents reported that confidential information is not given over the telephone SMS and IVR channels. Replies to queries received are issued by land mail to the registered address.

Key observations and findings for each channel

Internet

71. Table 11 provides a summary tabulation of the main types of data exchange security methods for services offered on the Internet channel. The methods are grouped under three main headings: SSL (which includes SSL and https (HyperText Transfer Protocol Secure) encryption), hash and Digital Certificates (which also includes PKI, electronic-ID and Electronic Signatures).

72. The table shows how revenue bodies use these different data exchange security methods to assure data confidentiality, data integrity and data non-repudiation, and how these relate to the services provided to taxpayers. The most frequently used technologies for the different assurances sought are:

    - Data confidentiality is generally assured by encrypting the message between the administration and the taxpayer using SSL.
    - Hashing is used to guarantee data integrity; whilst
    - Digital certificates are used to assure non-Repudiation – this is particularly relevant for the services to file a return and submit bank account details.

Table 11. Internet data exchange security methods for each service provided and used to assure data confidentiality, integrity and non-repudiation

Country	Service																								Overall strength of solution adopted as reported by the revenue body
	View tax account information			Amend taxpayer basic information			File a return			Amend return details			Submit bank account details			Make a payment			Claim repayments/ credits etc.			View confide-ntial info from revenue body			
	Which technologies do revenue bodies use for assurance of data: Confidentiality (**C**), Data Integrity (**I**) and Data Non-Repudiation (**NR**) Technologies are: SSL, Hash (H), and / or Digital Certificate (DC)																								
	C	**I**	**NR**	**C**	**I**	**NR**	**C**	**I**	**NR**	**C**	**I**	**NR**	**C**	**I**	**NR**	**C**	**I**	**NR**	**C**	**I**	**NR**	**C**	**I**	**NR**	
Australia	SSL	-	DC	SSL	-	DC	SSL	H	DC	SSL	-	DC	SSL	-	DC	-	-	-	SSL	-	DC	SSL	-	DC	Strong
Austria	SSL	SSL	SSL	SSL	SSL	SSL	SSL	SSL	SSL	SSL	SSL	SSL	SSL	SSL	SSL	SSL	SSL	SSL	SSL	SSL	SSL	SSL	SSL	SSL	Strong
Belgium	SSL DC	SSL DC	SSL DC	SSL	SSL	SSL	SSL	SSL	SSL DC	SSL DC	SSL DC	SSL DC	SSL DC	SSL DC	SSL DC	-	-	-	-	-	-	SSL DC	SSL DC	SSL DC	Strong
Canada	SSL	-	-	SSL DC	H	-	SSL DC	H	-	SSL DC	H	-	SSL DC	H	-	SSL	H	-	SSL DC	H	-	SSL DC	-	-	Adequate
Chile	SSL DC	H DC	-	SSL DC	H	-	SSL DC	H	-	SSL DC	H	-	SSL DC	H	-	SSL	H	-	SSL DC	H	-	SSL DC	H	-	Adequate
China	DC	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	Adequate
Denmark	SSL DC	-	-	-	-	-	SSL DC	SSL DC H	SSL DC	SSL DC	SSL DC H	SSL DC	SSL DC	SSL DC H	SSL DC	SSL DC	SSL DC H	SSL DC	-	-	-	SSL DC	-	-	Strong
Estonia	SSL	-	-	SSL	-	-	SSL	-	-	SSL	-	-	SSL	-	-	SSL	-	-	SSL	-	-	SSL	-	-	Adequate
Finland	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	
France	SSL	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	Adequate
Germany	SSL	-	-	-	-	-	SSL	H	DC	-	-	-	SSL DC	H	DC	-	-	-	-	-	-	SSL DC	H	-	Adequate/ Strong 1
Ireland	SSL	SSL	DC	-	-	DC	SSL	SSL	DC	SSL	SSL	DC	SSL	SSL	DC	SSL	SSL	DC	SSL	SSL	DC	SSL	SSL	DC	Strong
Italy	SSL	-	-	SSL	-	-	SSL	H	DC	SSL	-	-	SSL	-	-	SSL	H	DC	SSL	-	-	SSL	-	-	Strong
Japan	SSL	-	-	SSL	-	-	SSL	DC	DC	SSL	DC	DC	SSL	DC	DC	SSL	-	-	SSL	DC	DC	SSL	-	-	Strong
Korea	SSL	H	-	SSL	H	-	SSL	H	-	SSL	H	-	SSL	H	-	SSL	H	-	SSL	H	-	SSL	H	-	Strong
Mexico	SSL	-	-	SSL	-	-	SSL	DC	DC	SSL	DC	DC	-	-	-	-	-	-	-	-	-	-	-	-	Weak/adequate/ Strong 2
New Zealand	SSL	-	-	SSL	-	-	SSL	-	-	SSL	-	-	SSL	-	-	-	-	-	SSL	-	-	SSL	-	-	Adequate
Norway	-	-	-	SSL	-	-	SSL	-	-	SSL	-	-	SSL	-	-	-	-	-	-	-	-	SSL	-	-	Adequate
Portugal	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	
Singapore	SSL	H	-	SSL	H	-	SSL	H	-	SSL	H	-	-	-	-	SSL	H	-	SSL	H	-	SSL	H	-	Strong
South Africa	SSL	-	-	SSL	-	-	SSL	-	-	SSL	-	-	SSL	-	-	SSL	-	-	SSL	-	-	SSL	-	-	
Spain	SSL	H	DC	SSL	H DC	DC	SSL	H	DC	SSL	H DC	DC	SSL	H DC	DC	SSL	H DC	DC	SSL	H DC	DC	SSL	H DC	DC	Strong
Sweden	SSL	SSL	DC	SSL	SSL	DC	SSL	SSL	DC	SSL	SSL	DC	SSL	SSL	DC	-	-	-	-	-	-	SSL	SSL	DC	
Turkey	SSL	-	-	SSL	-	-	SSL	-	-	SSL	-	-	-	-	-	-	-	-	-	-	-	-	-	-	Adequate
USA	SSL	SSL	-	-	-	-	SSL	H DC	DC	SSL	H DC	DC	SSL	SSL	-	SSL	SSL	-	-	-	-	-	-	-	Adequate

Note: Statistics in this table are not mutually exclusive e.g. respondents that indicated that they use encryption but provided no further details are not included.

73. Table 11 also provides an assessment provided by revenue bodies for the overall strength of the solution currently in use by them. In general, there is no direct correlation between methods adopted and the strength indicated. Almost all the respondents indicated the same level of strength for all methods. This means that no matter what methods a respondent indicated, it stated the same level of strength for all methods across all services. The only exceptions are Germany and Mexico.

- Germany indicated that all methods are strong for all services except for confidential information sent by the revenue body to taxpayers, in the case of business customers, which was indicated as adequate.
- Mexico indicated that SSL is used for 'View Account' and 'Amend Taxpayer Basic Information' and while it is indicated as adequate for the first (i.e. View Account), it is indicated as weak for the second purpose (i.e. 'Amend Taxpayer Basic Information'). Digital certificates are used for 'File and Amend Returns' and are indicated as a strong method.

Securing data/document exchanges – findings and issues – Internet

Assuring data exchange confidentiality

- All 25 respondents offer secure electronic services on the internet, and of these, 22 replied to this question. Data confidentiality is almost always assured using one of a number of potential methods of encryption. The most common method used to assure confidentiality by 15/25 respondents is SSL 128 bit encryption. 128bit SSL is still regarded as an adequate level of encryption to satisfy data confidentiality. Some administrations advised that they use 256bit SSL which is the next encryption strength up from 128bit.
- Other specific responses included:
    - Singapore indicated that they use 128 bit encryption using a 2048 bit RSA key for the SSL cert. SLIFT and PGP[11] are used to encrypt the data in the case of backend server to server file transfers.
    - France reported that they use SSL AES (Advanced Encryption Standard) 256 bit.
    - Germany indicated they use SSL 128 bit encryption using 2048 bit RSA key for SSL cert.
    - Belgium reported that they assure confidentiality using SSL two ways with an ID card.
    - China reported that confidentiality is assured by using a digital certificate and username/password (digital certificate PKI can also be used to encrypt data for confidentiality).
    - Denmark indicated that they assure confidentiality using secure asymmetric encryption.
    - South Africa reported that they use HTTPS (this can be implemented using SSL128bit/256bit etc encryption) to secure confidentiality.

Assuring data integrity

- Twenty of 25 respondents replied to this question. Eleven respondents replied that they assure confidentiality by 'hashing' the data. Five of the 19 respondents that replied indicated that they assure data integrity using SSL (Australia, Austria, Belgium, Canada and Ireland).
- Other specific responses were that:

[11] RSA is an algorithm for public key cryptography. PGP (Pretty Good Privacy) and SLIFT are proprietary data encryption / decryption programmes

- Turkey indicated that data packets are compressed to 'zip' format.
- In addition to using SSL, Canada provided additional information advising that for the 'make a payment' service the latest 'hashing' algorithms are used. For all other services passwords are 'hashed' when stored, password entry is masked (*****), security questions and answers are encrypted for storage and directory changes are audited.

Assuring data non-repudiation

- Sixteen of 25 respondents replied to this question. A variety of methods were reported. Eight respondents advised that the use of digital certificates (PKI) identity authentication to assure against repudiation the transaction. Seven respondents advised that they use database logs and audit trails as a measure to assure non-repudiation of the transaction. Five of these advised that access to the backend database(s) is strictly controlled. Four respondents advised that they assure non-repudiation through the terms and conditions that a taxpayer accepts before using the service. Note: Not all of the respondents that use the terms and conditions use digital certificates e.g. France advised that they use a 'click and confirm' function on their website for customers who access the site using e-mail/password
- Other specific responses were that:
  - Austria and Belgium advised that they assure non-repudiation using SSL sessions.
  - Australia advised that they use database logs and terms and conditions. They also advised that when an Employee is filing a return, shared secrets are used for the first session and then a reusable complex password is issued for future sessions. Various unique identifiers are captured from the end-user during the lodgement process.
  - Ireland advised that in addition to digital certificate technology and database logs they use digitally signed electronic envelopes that contain all the taxpayer's transaction information. These electronic envelopes are stored securely and can be retrieved if identity or transaction content is challenged and are accepted as legally sound documents

Satisfaction with the overall strength of the solution being used

- Twelve respondents indicated that they consider the security measures they implement are strong. Another twelve consider the overall strength of their security measures for Internet services to be adequate.
- Some respondents reported that the strength of security differed between services ranging from weak to strong.

Issues identified and solutions planned or implemented

- Some issues were reported relating to the provision of services on the internet but none specifically to do with the data confidentiality, data integrity and data non-repudiation.

Securing data/document exchanges – secure e-mail

Assuring data exchange confidentiality

- Seven of 25 respondents advised that they offer services on this channel, and of these five replied to this question.
- Specific responses were that:
  - Australia, New Zealand and Singapore advised that secure e-mail is accessed through their online portal and therefore uses SSL 128 bit encryption.
  - Ireland advised that they use SSL for inbound mail and outbound mail is encrypted using 192bit key strength

Assuring data integrity

- Four of the eight respondents that offer services using secure e-mail answered this question.
- Specific responses were that:
    - Australia advised that services directly read and write to and from the Australian Tax Office core systems in real time and that all interactions occur within the secure online session.
    - Ireland advised that they assure data integrity by using SSL for inbound mail and encrypting outbound messages with AES 192 key strength.
    - New Zealand advised that they have no systems in place to assure data integrity.

Assuring non-repudiation

- Five of the eight respondents that offer services using this channel replied to this question.
- Specific responses were that:
    - Australia, Denmark and Singapore advised that secure e-mail services are accessed via their online portal. Australia also indicated that non-repudiation is also assured through database logs.
    - Singapore advised that all secure e-mail threads are stored and are visible on the online portal. A personal ID number and/or the company's ID number and a PIN are required to use the service.
    - Ireland reported that a taxpayer must use a password to transact on the secure e-mail service. The password is then associated with the secure e-mail transaction to assure non-repudiation.
    - New Zealand indicated that customers require a personalised secure logon and password in order to use secure e-mail.

Satisfaction with the overall strength of the solution being used

- There were four responses to this question.
- Specific responses were that:
    - Australia and Singapore both indicated that the security measures they use are strong.
    - Ireland and New Zealand reported that their measures are adequate.

Issues identified and solutions planned or implemented

- Australia advised that their secure e-mail service had a message limit of 4,000 characters and that their lodgement/amendment details must be keyed in by tax office staff, which poses a risk regarding data integrity. This problem has been somewhat alleviated by accepting attachments to mails received. Data entry measures have also been introduced.
- New Zealand highlighted their dependency on upfront identity assurance checks which could be alleviated by adopting a whole-of-government solution.

Securing data/document exchanges – standard e-mail

Assuring data exchange confidentiality

- Six of 25 respondents offer this channel. Four respondents out of the nine that offer services using standard e-mail replied to this question:

- New Zealand advised that they assure confidentiality through Terms & Conditions but encourage the taxpayer to use secure e-mail.
- The USA advised that replies to queries received on standard e-mail are deposited on an online system. Therefore they assure confidentiality through using SSL 3.0 128 bit encryption
- Singapore and Ireland advised that customers are directed to use secure e-mail for confidential queries.

Assuring data integrity

- Singapore advised that data integrity is assured as replies to queries received are deposited on their online portal or issued by land mail to the registered address.
- USA advised that replies are deposited on an online portal known as SOR. An e-mail is sent to the taxpayer alerting them that data has been deposited. They have a limited amount of time to access the reply before it is automatically deleted.

Assuring non-repudiation

- Most respondents advised that the channel is used to receive information however sensitive information is returned using other channels:
  - Belgium advised that a business individual must include a reference number and a unique company code that is issued by land mail. An Employee includes their reference number that is comprised of their National ID number and another unique reference number.
  - Ireland advised that customers are advised to use secure e-mail for sensitive data. Copies of standard e-mails are retained. Replies are issued by land mail to the registered address.
  - Singapore advised replies are either deposited on their online portal or sent by post to the registered address.

Issues identified and solutions planned or implemented

- The only issue reported for standard e-mail was its inability to assure data confidentiality. No solutions were offered other than to use a different channel or a secure e-mail channel.

Securing information exchanges – telephone voice

Assuring information exchange confidentiality

- Fifteen of 25 respondents offer this channel. Seven of the 15 respondents that offer this service replied to this question:
  - Six respondents (Australia, Canada, Germany, Ireland, New Zealand and the USA) advised that they perform a 'proof of identity' assessment before a confidential conversation is initiated e.g. taxpayers unique revenue number, national ID number or shared secrets from taxpayer records.
  - Singapore reported that replies that contain confidential information are either deposited on the online portal or issued by land mail to the registered address. Replies can be communicated over the phone only if the identity or relationship of the caller to the business can be ascertained.

Assuring data integrity

- Five of 15 respondents that offer this service replied to this question. Some replies referred to the integrity of the data available to staff when dealing with telephone queries.
  - Ireland advised that the proof of identity is checked to establish the identity of the caller through data matching a number of shared secrets. If any doubt

arises during the call as to the authenticity of the caller the call will be terminated and a return call will be made using the telephone number on file or communications will be initiated by land mail to the registered name and address on the administration's records

- Singapore advised that replies can be communicated over the telephone only if the identity or relationship of the caller to the business can be ascertained.
- The USA advised that they establish the identity of the caller through data matching answers to a number of shared secrets. They have both standard questions and high-risk questions. High risk questions are more detailed and answers would be more difficult for a caller to obtain. If doubt arises about the identity of the caller the call will be terminated and any changes made communicated by land mail to the registered name and address.

Assuring non-repudiation

- A small majority of the 15 respondents that offer services using this channel replied to this question. Most respondents rely on the strength of the verbal challenges policies in place in their administration:
  - The USA advised that any changes made, as a result of telephone voice instructions, are notified to the registered taxpayer by land mail at the address on file.
  - Australia, New Zealand and Ireland advised that they record telephone voice calls.
  - Canada advised that they rely on the strength of the registration process and integrity of other areas with the Canada Revenue Agency.
  - Ireland and the USA reported that a call is terminated if any doubt arises as to the identity of the caller. Voice calls are also recorded.

Satisfaction with the overall strength of the solution being used

- Six respondents advised that they considered their security measures for services provided to be adequate; Australia advised that they considered the security measures they have implemented to be strong.

Issues identified and solutions planned or implemented

- There were no issues reported.

Securing data/document exchanges – telephone SMS

Assuring data exchange confidentiality

- Five of 25 respondents offer services using this channel. Three of the five respondents replied to this question. All three use data encryption, with or without other measures, to assure data confidentiality.
  - Chile and Ireland advised that they assure confidentiality by the strength of the access token (Chile - ID/password, Ireland PPSN+PIN/Registration number) and also by SSL 128 bit data encryption. Ireland also advised that the service provider encrypts the data transmission between the taxpayer and Revenue systems.
  - Singapore advised that no confidential information is given out to taxpayers using SMS and that files are encrypted using SLIFT/PGP when transmitting taxpayers' details over to the SMS service provider.

Assuring data integrity

- There were three responses to this question.
  - Chile advised that they assure data integrity by hashing the message

- Ireland advised that the customer must provide proof of identity (shared secret) and the service provider encrypts the data transmission between the taxpayer and Revenue systems.
- Singapore advised that they assure data integrity by using control totals where applicable when transmitting data flow to the SMS provider.

Assuring non-repudiation

- There were only four responses to this question.
  - Ireland advised that the service can only be accessed using shared secret information (PPSN and PIN) between the administration and the taxpayer. The contact number from which the request was received is automatically recorded and retained. No confidential information is returned using SMS and is sent via land mail.
  - Singapore advised that files are either sent to the SMS service provider through server-to-server connections or via courier.
  - Spain advised that they assure non-repudiation by retaining the SMS.
  - Turkey noted that only unclassified data is exchanged using SMS.

Satisfaction with the overall strength of the solution being used

- All five respondents that offer services using SMS consider the security measures to be adequate.

Issues identified and solutions planned or implemented

- There were no issues reported.

Securing data/document exchanges – telephone IVR

Assuring data exchange confidentiality

- Eleven of 25 respondents offer services using this channel. Seven of the 11 respondents that offer services using telephone IVR replied to this question. Most advised that limited services are available using this channel:
  - Five respondents (Australia, Canada, Ireland, New Zealand and the USA) advised that they establish the identity of the caller by matching customer information/shared secrets against Revenue records. Replies are then issued by land mail to the registered address.
  - Chile advised that they assure data confidentiality by using SSL 128 bit encryption and establish the identity of the caller by ID/password.
  - Singapore advised that no confidential information is disclosed over this channel. Replies to queries are either deposited on the online portal or sent via land mail to the registered address.

Assuring data integrity

- Five of the 11 respondents that offer this service replied to this question.
  - Chile advised that they assure data integrity by hashing the data.
  - Australia advised that they use shared secrets and real time checks to the Australian Tax Office systems.
  - Canada advised that access to data in directories is restricted to view only and upon retrieval of data they verify that the data is of an expected format.
  - Singapore advised that no information is given out on this channel. Instead replies are either deposited on the online portal or issued by land mail to the address on record.

Assure non-repudiation

- Seven of the 11 respondents that offer services using telephone (IVR) replied to this question.
    - Australia advised that they assure non-repudiation through standardised proof of identity requirements and that all calls are recorded.
    - Canada advised that the authentication process and user access is recorded, logged and audit trailed at every step. Strict system access controls apply for access to any data logs.
    - Ireland advised that any data updates arising from calls are logged and strict access rights to the database are enforced. Requests to change address are dealt with manually and may require proofs. Where a reply is necessary it is issued by land mail.
    - Spain advised that it is possible to rebuild the data that has been keyed by the taxpayer.

Satisfaction with the overall strength of solution being used

- Eight of 11 respondents that offer the service advised that the security measures they implement are adequate.

Issues identified and solutions planned or implemented

- There were no issues reported.

Securing data/document exchanges – intelligent mobile devices

Assuring data exchange confidentiality and data integrity

- Two out of the four respondents that offer services using intelligent mobile devices replied to this question:
    - Ireland advised that data confidentiality and integrity is assured using SSL 128 bit encryption.
    - The USA advised that they hash the message to assure confidentiality and data integrity.

Assuring non-repudiation

- Two out of the four respondents that offer services using intelligent mobile devices replied to this question:
    - Ireland advised that the service is accessed using a PPSN, PIN and another shared secret.
    - The USA advised that this channel is used to provide the customer with a date in relation to a refund.

Satisfaction with the overall strength of the solution being used

- Two out of the four respondents that offer services using intelligent mobile devices replied to this question:
    - Ireland advised that the security measures they implement are strong.
    - The USA advised the security measures they implement are adequate.

Issues identified and solutions planned or implemented

- Ireland advised that there have been issues with intelligent mobile telephones not recognising the issuing Certificate Authority for the SSL certificate.

V. LEGAL FRAMEWORKS

74. The final area of the study examined the legal frameworks and certificate policy and practice statements, in use and tested in administrations that provide a legal framework to support identity authentication, data confidentiality, and non-repudiation of identity or the integrity of data content. The survey posed the following questions:

1) Does your administration have a legal framework supporting identity authentication? Describe.

2) Does your administration have a legal framework supporting data confidentiality? Describe.

3) Describe how your legal framework supports non-repudiation i.e. challenges by a taxpayer as to identity or the integrity of data content?

Key findings

- The majority of respondents (21/25) indicated that their administrations have legal frameworks[12] supporting identity authentication – see Table 12.
- The majority respondents (23/25) indicated that they have legal frameworks supporting data confidentiality. In most cases the legal framework involved a combination of national and tax legislation (as well as policies and procedures operated by the tax administrations) – see Table 12.

Table 12. Existence of legal frameworks supporting identity authentication, data confidentiality, and non-repudiation of identity or the integrity of data content

Country	A legal framework exists to support identity authentication	A legal framework exists to support data confidentiality
Australia	Yes	Yes
Austria	Yes	Yes
Belgium	Yes	Yes
Canada	No	Yes
Chile	Yes	Yes
China	Yes	Yes
Denmark	Yes	Yes
Estonia	Yes	Yes
Finland	Yes	Yes
France	Yes	Yes
Germany	Yes	Yes
Ireland	Yes	Yes
Italy	Yes	Yes
Japan	Yes	Yes
Korea	Yes	Yes
Mexico	Yes	Yes
New Zealand	No	Yes
Norway	Yes	Yes
Portugal		
Singapore	No	Yes
South Africa	Yes	Yes
Spain	Yes	Yes
Sweden	Yes	
Turkey	Yes	Yes
USA	Yes	Yes
Total (Yes)	21/25	23/25

[12] In certain cases where respondents have indicated that there was a legal framework in place that supported identity authentication, they provided information only in relation to policies and practices. In such cases, it is assumed that the legal framework referred to by the respondents underpins the policies and practices described.

- Survey responses suggested that respondents use different ways to protect against repudiation of a transaction by a taxpayer based on either identity or the integrity of data content. Some respondents use administrative policies to ensure a direct audit trail of evidence from taxpayer to the administration. Some use non-filing penalties to address taxpayers who deny filing a return transaction or deny some of the content. A number of respondents made direct reference to having legislative provisions in place to protect against repudiation of a transaction by a taxpayer based on either identity or the integrity of data content.

The use of legal frameworks to support identity authentication

- The majority of respondents (21/25) indicated that their administrations have a legal framework supporting identity authentication:
    - France advised that there is a national (whole-of-government) legal framework in place in relation to security for public administration e-services. This framework defines the rules each security function (authentication, confidentiality, electronic signature, timestamp) must conform to, depending on the security level required.
    - Korea advised that they have a national legal framework in relation to security for e-services of public sector and of private sector. This legal framework has the regulations for each security function (authentication, confidentiality, integrity, electronic signature, timestamp, etc). All e-services must conform to the regulations. This also supports data confidentiality (see below).
    - Two respondents, Canada and New Zealand, advised that although they have no legal framework in place supporting identity authentication, they have policies, practices and processes in place in this area.

Box 4. The legal framework supporting identity authentication in USA

National legislation mandates that a Privacy Impact Assessment be performed for Federal/State agencies' computer systems containing PII. (PII is one or more pieces of information that when considered together or when considered in the context of how it is presented or how it is gathered is sufficient to uniquely identify a specific individual.) An enterprise privacy risk assessment methodology shall be implemented at the programme level to ensure the appropriate mitigation of identified privacy risks. Risk assessments provide assurance levels commensurate with sensitivity of data/transaction type. In addition, technical guidance is available from a state technology agency, which defines different levels of assurance in terms of the consequences of an authentication error.

The use of legal frameworks to support data confidentiality

- The majority respondents in this area (23/25) indicated that they have legal frameworks supporting data confidentiality. In most cases the legal framework involved a combination of national and tax legislation (as well as policies and procedures operated by the tax administrations).
    - Korea (as noted in Section above regarding identity authentication) advised that they have a national legal framework in relation to security for e-services of public sector and of private sector. This legal framework has the regulations for each security function (authentication, confidentiality, integrity, electronic signature, timestamp, etc). All e-services must conform to the regulations.
    - France (as noted in Section above regarding identity authentication) advised that there is a national (whole-of-government) legal framework in place in relation to security for public administration e-services. This framework defines the rules each security function (authentication, confidentiality, electronic signature, timestamp) must conform to, depending on the security level required.
    - Singapore noted that they have secrecy provisions in the Tax Acts to govern and preserve the confidentiality of data, as well as a Data Administration Policy that prescribes how data is to be stored, managed and administered. Different levels of security standards and controls are applied to different classifications of data,

with the most stringent controls applied to data classified as 'Top Secret' or 'Secret', and the least stringent controls applied to 'Unclassified' data. Other classifications include 'Confidential' and 'Restricted'.

How legal frameworks support non-repudiation i.e. challenges by a taxpayer as to identity or the integrity of data content

- Revenue bodies' use different ways to address data integrity and non-repudiation. Some use administrative policies to ensure a direct audit trail of evidence from taxpayer to the administration. Some use non-filing penalties to address taxpayers who deny filing a return transaction or deny some of the content. A number of respondents made direct reference to having legislative provisions in place to protect against repudiation of a transaction by a taxpayer based on either identity or the integrity of data content.
    - Canada – the only legal framework that might support non-repudiation are the policies pertaining to management of records and data and internal audit trails of system accesses. (The same respondent noted that although there was specific legislation in this area, it only applied to PKI based transactions. However, the tax administration (CRA) does not use PKI technology for taxpayer transactions over the Internet.)
    - France – the framework in place to solve issues related to non-repudiation is based on the filing obligations on a taxpayer and the fact that a taxpayer can be surcharged for not having filed a return in the event that s/he challenges the fact that s/he filed a particular tax return.
    - Ireland – has national legislation (the Electronic Commerce Act, 2000) supporting the admissibility of an electronic form of a document and an electronic signature. The legislation states that nothing in the application of the rules of evidence shall apply so as to deny the admissibility of an electronic form of a document in evidence. The legislation also provides for electronic communication to contain an electronic signature, an advanced electronic signature, an electronic signature based on a qualified certificate, an electronic signature created by a secure signature creation device or other technological requirements relating to an electronic signature. The legislation assures that a signed electronic document cannot be repudiated based on identity or content.
    - Italy – legal framework in relation to non-repudiation is contained in a section concerning digital signature in the Code on Digital Public Administration, which implemented the Directive 1999/93/EC of the European Parliament and of the Council of 13 December 1999 (on a Community framework for electronic signatures).
    - Japan – according to legislation in relation to the online filing and payment system, when electronic signatures are used directly by the relevant individuals for electronic data, the data in question is assumed to have been established as authentic.
    - Korea – The regulations for digital signature and timestamp support non-repudiation in the case of transactions using digital certificate. In the case of using ID and password, we have the policies using internal audit trails of taxpayer's system accesses.
    - Mexico – taxpayers are obliged to send information signed with a Digital Certificate.
    - Singapore – the non-repudiation of identity authentication and data content is provided for in specific tax legislation, once an authentication code (password or PIN) has been assigned to a taxpayer. In the case of individuals, both the SingPass* and the IRAS** PIN are tied to their unique Identity Number. Authentication is based on the unique combination of their Identity Number and their SingPass or IRAS PIN. In the case of businesses, only staff who have been properly authorised by the business via IRAS EASY (e-Services Authorisation System) authorisation and authentication system can transact online on behalf of the business. IRAS e-services check that the staff member is an authorised person

before allowing the person to access the e-services. *SingPass Singapore Personal Access **Inland Revenue Authority of Singapore

- Spain – the use of an electronic signature is their mechanism for supporting non-repudiation.
- Turkey – relies on transaction logs, which cannot be altered, to support non-repudiation
- USA – have a legislative provision that states that the fact that an individual's name is signed to a return, statement, or other document shall be prima facie evidence for all purposes that the return, statement, or other document was actually signed by him/her.

VI. KEY FINDINGS AND RECOMMENDATIONS

75. The preceding chapters have provided a fairly comprehensive description of revenue bodies' approaches to meeting security and authentication requirements for the main services provided by their electronic service channels for their main taxpayer groupings.

76. The key findings and recommendations from this study are as follows:

Overall developments

- It is noteworthy that despite the steady growth in the range and uptake of electronic services in taxpayer services, the most widely used security and authentication technologies have remained largely unaltered over the past decade. The issues surrounding the management and maintenance of many of these – digital certificates, PIN numbers, passwords, tokens and code cards – are well known by all revenue bodies, yet at present there still appear to be few established alternatives. The current experience with new technologies which offer the promise to prevent or reduce these issues –such as biometrics, or the use of cloud computing in areas such as the management of digital certificates– is very limited, but these innovations are just appearing on a small number of revenue body agendas, and may warrant investigation to update this report once they have become more mature.

The national context

- A significant majority (80%) of revenue bodies contributing to this research are able to benefit from the existence of a **national identity register** to aid them in identity authentication, and countries have identified many advantages from this, benefiting both the administration and customers, whilst identifying no disadvantages. A smaller percentage (48%) of governments go further and provide a **national identity authentication service** , enabling government departments and agencies to share the benefit of a service built once rather than many times within a country, and taking complexity for customers out of interactions with government. This reduction in complexity also reduces the administrative burden of compliance, which is a strategic goal in many revenue bodies. In addition to the 48% who currently benefit from a national identity authentication service, another 20% of countries report having such a service planned. This **whole-of-government approach** offers significant benefits to both the service provider and its customers.
- Benefits cited for the ability to use a national identity register include:
    - Provides an authoritative and certified source of identity data
    - Provides efficiencies in assisting the identification of taxpayers
    - Reduces administrative work
    - Avoids replication
    - Facilitates the sharing of identity information between different departments and public bodies
    - Facilitates the re-use of data
    - Reinforces the mechanism for identity proof and standardises the process
    - Provides an additional security level
    - Customer service benefits were also noted, such as avoiding the need to contact taxpayers and providing a simpler and more streamlined system for taxpayers and administrations.

Third party authentication services

- A significant minority (48%) of countries use a **trusted third party authentication service**. These countries cite benefits including savings to the tax administrations in

terms of financial and human resources and efficiencies; opportunities to reach a wider number of potential e-Service users; high level of satisfaction with the authentication method and level of performance of the third party; taxpayer convenience; savings for business and government; and easy and secure access for parties involved

- No issues were reported related to the fact that the authentication service was provided by a third party.

First registration with the tax authority

- Almost all countries (79%) use identity proof information from a national or private third party identity register for new taxpayer registrations. In most cases, **employees** register with the tax administration using their social insurance number or equivalent or a national ID document. Some administrations advised that they offered a number of options to an employee seeking to register. For **business corporate taxpayers**, the main types of identity information proofs are registration information from the Companies Office, including certificate of incorporation, and information on any Directors of the company, information from business regulatory authorities, face-to-face business visits. For **business individual taxpayers**, the main types of identity information proofs advised were Business Number issued by the regulatory authorities, personal social insurance numbers, identity proofs from local registers of residents, date of birth or photo identification. Finally, **tax intermediaries**, all countries facilitate the use of tax intermediaries (see footnote 1, page 7). Some are quite flexible about the type of person that will be accepted as an authorised advisor. This can range from a family member to lawyers, tax practitioners and professionals with qualifications through a professional association. In other countries, tax intermediaries are regulated and must have a recognised professional qualification and or be a member of a recognised professional association. To register a tax intermediary with the revenue body, eight countries advised that the tax intermediary must provide a national ID as proof of identity, whilst for six proof of an agent's professional qualification through a professional association is required.
- Regarding the **channels** used to provide secure electronic services, the Internet is by far the most widely used channel. This report considered eight typical services across four customer groups and 25 participating countries, giving a total potential 800 service offerings.
    - Of **current services**, the Internet is used for 562/800 service offerings and is by far the most mature; telephone (voice) at 158 and secure e-mail at 136 and at the second highest level of maturity; IVR at 69 is relatively immature; and telephone (SMS) and intelligent mobile devices at 19 and 8 respectively are both quite embryonic. Although used for 61 service offerings, standard e-mail can be considered mature but of limited use in the context of secure electronic interactions, and this is not likely to change unless security features (making this more akin to secure e-mail) are built into the products by software providers, and that this becomes the norm.
    - For **planned new services**, the picture is quite different, with 39 new service offerings planned for intelligent mobile devices, 36 for secure e-mail, 20 for telephone (IVR), 16 for telephone (voice), 12 for the Internet, and none for either telephone SMS and standard e-mail. If these planned new service interactions are all implemented over the course of the next two years, they will have a relatively modest impact overall on the significance of the various channels in the strategies of the participant revenue bodies with two exceptions: secure e-mail will become as significant as telephone (voice) as the tie second most important channel; and the use of telephone (SMS) will fall below intelligent mobile devices into the position of channel of least significance.
- The primary **identity authentication methodology** in use by most administrations has a common pattern to it i.e. effectively establish the identity of the taxpayer or tax intermediary from the outset and issue an access token to the identified taxpayer or intermediary for use in connecting to secure electronic services.

- There is considerable consistency regarding the **technology (tokens)** used for accessing the secure services with almost all respondents providing access to their secure electronic services using a variety of systems/tokens. The most common systems/tokens used are one or a combination of the following: Digital Certificate, User ID, PIN and Password. Other tokens used include Code Card, Electronic ID card, Shared Secrets/tax records and National ID. A number of administrations offer a Digital Certificate that can be used on a smartcard, mobile phone, security stick or soft PSE.
- Some revenue bodies are re-considering their continued use of digital certificates, on the basis of their negative impact on the uptake of electronic services, combined with the relatively high cost of administering them.
- Only three respondents reported that they used biometrics as part of their identity authentication, and the use of this technology should be considered quite embryonic in this context.
- In terms of the **services offered to the four customer groups** studied (employees, business corporate, business individual and tax intermediary), there is remarkably little variation in the total number of service offerings, at 248, 245, 254 and 228 respectively (all out of a total possible of 1,344 – eight services, seven channels and 25 countries).
- Almost all respondents use the common widely used SSL data encryption to assure **data confidentiality** for data exchange by internet. This SSL system continues to provide the best solution for tax administrations.
- **Data integrity** is mainly assured by hashing the data. In general, the majority of respondents indicated hashing to be of at least adequate strength. Digital Signatures using Public Key Infrastructure (PKI) can also be used to provide data integrity checks.
- There is more variety in responses in relation to assuring data **non-repudiation**. Replies included using digital certificates, database logs, terms and conditions or shared secrets. The overall strength of these methods is considered by respondents to be at least adequate.
- Most countries (83%) have **legal frameworks** supporting identity authentication, and slightly higher (92%) have legal frameworks supporting data confidentiality. In most cases the legal framework involves a combination of national and tax legislation, as well as policies and procedures operated by the tax administration. Countries use different ways to protect against repudiation of a transaction by a taxpayer based on either identity or the integrity of data content; some use administrative policies to ensure a direct audit trail of evidence from taxpayer to the administration, some use non-filing penalties to address taxpayers who deny filing a return transaction or deny some of the content, and a number have legislative provisions in place to protect against repudiation of a transaction by a taxpayer based on either identity or the integrity of data content.

Recommendations

- *Adopt a whole-of-government approach where feasible:* Revenue bodies should support government services or plans for the establishment of national identity registers and national identity authentication services, and make full use of these where they exist.
- Revenue bodies not able to use a government national identity authentication service may wish to consider the use of a trusted third party service. This report provides details of which other countries have successfully adopted this approach, and of the benefits which they have identified.
- Revenue bodies should continue to monitor both customer demand and channel maturity for electronic service delivery in other sectors, as the relative significance of the different channels could change quite markedly even over the short and definitely over the medium term.
- Revenue bodies reviewing their own channel strategy or technology strategy for the delivery of secure electronic services should consider liaising with peers –identified in this report– who have already adopted the aspects they are considering, especially (with respect to technology strategy) in relation to digital certificates and biometrics.

Annex 1. Detailed responses to questions on national identity register

Question 1. Do you have a national identity register run by central government or a government department?

Australia	We have a central government register for business but do not have a national identity register for individuals. There is a strong privacy culture and a strong legal framework in Australia. The legal framework protects Australians from having their information shared by private organisations as well as government.
Chile	Business register is managed by the tax administration.
Germany	Although individual identity registers are managed at local level/community level, data from the registers is sent to the central federal tax office. Local courts manage business registers.
Italy	Local/municipal authorities are responsible for the identity register, but in this case, the municipal registry offices are connected by a national index. The municipal registers register and assign tax codes to citizens. The main registry for businesses is the Companies Registry. The Chambers of Commerce are responsible for registration and assigning tax codes to companies.
Mexico and Spain	There is no single national business registry in their jurisdictions.
Singapore	Identity registers are managed by various bodies: the registers for citizens and permanent residents are maintained by the Immigration and Checkpoints Authority, while those of foreign workers are maintained by the Ministry of Manpower; the identity register for businesses is maintained by the Accounting and Corporate Regulatory Authority.
Sweden	Tax administration manages the population register. A separate body manages the business register.
South Africa	Separate government departments manage the individual and business identity registers.

Question 2. If no to Q1, why do you not have a national identity register?

Ireland	The Companies Registration Office maintains a national business register for corporate business but that the register does not include non-corporate businesses. The tax administration maintains its own combined corporate and non-corporate business register. The Department of Social Protection maintains a register of individuals. It is not shared at a national level but the register data is available to the tax administration. The tax administration and the Department of Social Protection also share a common identity number for the individual called a Personal Public Services Number (PPSN).
Italy	Municipal authorities are responsible for the registration of individuals. The municipal registers also hold the tax codes, which are assigned to citizens by the tax administration. However, in this instance, the municipal registry offices are connected by a national index.

Question 3. What identity proofs are required for individuals when registering on your national identity register?

Denmark	The entry of a birth in the parish register is considered legal proof of identity for registration in the national identity registry (the Civil Registration System). Immigrants requiring a personal identification number must provide a passport or other legal picture ID, a hiring contract and a work permit;
Denmark, Norway and Singapore	Specific identity proofs are required of individuals other than citizens.
Korea	The Ministry of Public administration and Security is operating national identity register system for citizens. Municipal authorities use this system to register individual identity for

	citizens. By law, citizens must submit an application form and a birth certificate to municipal authorities at birth. Municipal authorities use such information to register individual identity for citizens. Individual identity number for citizens consists of six digits for birth date and seven digits for additional information. Individual identity resister for foreigners is managed by the Immigration Service. By law, foreigners who stay more than 90 days or have another reason to resister must submit an application form, a copy of passport, a photograph, and if necessary, additional certificates to the Immigrant Service. Individual identity number for foreigners also consists of six digits for birth date and seven digits for additional information like domestic individual identity number.
Mexico	The national population register issues a unique population registration key directly or through a related third party. They advised that applicants seeking registration to the national identity register (the National Population Register) must attend a service module in addition to submitting proof of identity documents such as photo ID and birth certificate.
Norway, Estonia, Singapore and Sweden	Registration to the national identity register is carried out automatically at birth
Norway	Foreigners must provide a passport or driver's licence and a copy of register data from the national identity register in their home country
Singapore	Different identity proofs are required for each of the following category of individuals; naturalised citizens, permanent residents, and foreigners. The identity proofs required for these groups of individuals include an identity card, birth certificate and passport or travel documents. Depending on the individuals' circumstances, additional documents relating to areas such as employment, salary, marital status, income tax, financial information and so on were required.

Question 4. What identity proofs are required for business when registering on your national identity register?

Australia	Official company creation details, previous registration details (if any), business contact details and identity details of individuals who can legally bind the business
Austria	Photo identification (passport, personal ID card) of involved persons is required (as well as a contract of establishment of business).
Belgium	Official company creation documents signed by company representatives and a registered notary must be submitted with an application for registration. Similarly, Germany advised that a notarised application for registration is required.
Chile	Personal information of the partners and identification of legal representatives, in addition to a certificate of the company registration at the Register of Commerce and information regarding the business.
Denmark	The signature and personal ID number of the person registering the company are required (either in paper format or via a digital service where the persons signs with his/her personal digital signature). In the case of associations or partnerships, the contract of the partnership or the articles of association is required.
Korea	National identity register for businesses is managed by the National Tax Service. For business identity register, an application form, a copy of personal identification (national id-card, driver license, passport, etc) and signature of the person submitting an application and of representative, if necessary, corporation register number (the corporation register is managed by Ministry of Justice), a copy of business certificate, of lease contact, of the architectural drawing of the leased space, etc must be submitted to the National Tax Service by law. Business identity number consists of three digits for displaying tax office which register the business identity, two digits for displaying business type, and five digits for additional information.
Mexico	The person representing the corporation must present his/her own proof of identity and documentation proving their legal personality for the corporation.
Norway and Singapore	A greater level of identity proofs is required for business.

Norway	The social security number of the CEO and members of the board are required, as well as the organisation number of the accountant (tax intermediary) and auditor. The CEO or accountant must sign the application document and if submitted electronically, this must be done through the government eService.
Singapore	In the case of companies, the identity proof information required for registration includes the following: name, address, ID number and ID type of applicant; name, address, ID number, ID type, and nationality of proposed director and proposed subscriber; as well as company details. The identity proof information required of sole-proprietorships and partnerships includes the following: business name, contact details and ID card number or employment pass number of the owner/manager; and details regarding the business.
Sweden	The personal ID number and signature of the person submitting the application form (either in paper or electronically) is required. Sweden was the only country to note specific requirements in the case of foreign owners who are resident abroad, who must identify themselves with a certified copy of their passport.

Question 5. If you have a national identity register and you do not use the service, why not?

France	Although the tax administration uses the national identity register for individuals, it is only used indirectly, in back-office processes (e.g. to complete and verify consistency of individual taxpayers registry, or to exchange data between social administrations and the tax administration). A mapping table between individual taxpayer number and their national identity number is thus maintained (through name/date of birth/place of birth recognition), but is used with very strict and controlled rules. This table cannot be used directly by tax employees, nor can it be used for e-services identification.
Japan	The tax administration is not permitted to use the national identity register directly for individuals. However, they indirectly use the national identity registers for individuals and businesses in obtaining electronic signatures and electronic certificates which are required when using the tax administrations electronic filing and payment system.

Question 6. What are the benefits to your tax administration from having a national identity register?

Australia	Enables us to re-use the information to streamline the registration for an authentication credential.
France	The national identity register allows the sharing of the same identifier (only in relation to business information) between the tax administration and other public administration and also private partners.
Korea	The burden of tax administration is reduced in terms of financial and human resources. Identity is managed uniquely. It is easy to identify taxpayer.
Sweden	Everyone who lives in Sweden is registered in the population register (folkbokföring). The register contains details on all who live in Sweden and where they live. Population registration is one of the tasks of the Tax Agency. The aim of population registration. Population registration is very important to you. The fact that you are registered, and where you are registered, affects many of your rights and obligations, including the right to child allowance and health insurance. Population registration also allows you to prove your identity and family circumstances, etc., by means of a population registration certificate (personbevis) and other extracts from the records. An important task of the population registration service is to ensure that society has up-to-date information on the population. Information is passed on to other official bodies from the Tax Agency's population registers. Information in the registers. The tax office records incoming cases in the population register. Details such as name, address, date of birth, family circumstances and place of residence is registered for each individual. Everyone registered in Sweden is given a national identity number (personnummer) consisting of the date of birth (yy/mm/dd) followed by a four-figure number for each individual.

Question 7. Does the tax administration supplement the national identity register with its own additional data? If yes, why?

Australia	Used to support proof of identity checks for registered representatives of a business, and for additional checking where an identity is uncertain.
Belgium	The tax administration uses a unique tax administration specific identifier for individuals, because the national identity number for individuals (used for the national identity register) could change under certain special cases according to national law.
China	Add a six-digit number to the identity code for businesses in order to indicate the province, city and county where the business is located.
Denmark	Store certain additional personal data required for the correct computation of tax liability.
Korea	We supplement individual identity register with additional code for discerning taxpayer types (organization which is considered as resident, corporation type, V.A.T type, etc)
Singapore	Some taxpayers are not included on any national identity register (e.g. clubs and associations), thus requiring the tax administration to supplement with its own identity numbers for these taxpayers.
Spain	Stores certain alternative business address information.
South Africa	The tax administration acts as the intersection of multiple sets of third party data and needs to cross reference and augment identity data and maintain multiple security roles and rights and 'tax product' relationships that would not be in the domain of any other identity register.
Turkey	Stores a unique tax identity number (VKN), which is related to the national identity number (TCK).

Question 8. Is a national electronic identity authentication service provided for your tax administration? If yes, how does this operate?

Australia	The Australian Taxation Office (with another agency) manages a whole-of-government authentication service for business to government and government online interactions.
Austria	National electronic identity authentication service is operated via a certification company and uses digital signature card and mobile phone identification.
Chile & Ireland	There is no national electronic identity authentication service provided in their jurisdiction and that the tax administrations had developed their own electronic systems.
Estonia	A single national certification authority provides certificates for authentication and digital signing to national ID cards. This authority operates authentication via an ID card and card reader.
Finland	The People's registration centre offers all person identities but their e-service is based on voluntary Smartcards certificates and only a small minority of people do have them. Instead of that the Netbank Identity services are the practical solution. The Tax Office of Finland run the national electronic identity service of businesses and also extend this service to other branches of government.
Germany	In 2010 a national personal identity card with a personalised e-identification and signature functions was introduced. The ID card chip can transmit required data using secure encrypted connections as soon as the cardholder authorises such transmission by entering a PIN. Authorisation certificates control which personal data may be transmitted to providers of Internet applications and administrative services. They noted that the new ID card increased security as users must not only know the six-digit PIN but also be in possession of the ID card.
Japan	The national identity registration system uses dedicated lines and firewalls, mutual authentication between correspondents, data encryption and analysis, etc. using Intrusion Detection System. Efforts are also made to ensure the stability of this system through developing facilities necessary to safeguard against disasters as well as installing back up lines. The tax administration indirectly uses the national identity register to obtain electronic

	signatures and electronic certificates.
Norway	An authentication service is available for all public services.
Singapore	Individuals can apply for a personal access PIN number tied to their unique identity number and these two numbers can be used across government agencies' e-services to uniquely identify and authenticate individuals. A third-party service provider operates the personal access PIN number. When an individual logs on to a government e-service, s/he is directed to the logon page of this service for authentication, before being redirected back to the e-service for her/his transaction.
Spain	Electronic national ID card has a digital certificate that can be used as a proof for authentication. In addition, individuals and businesses can use other digital certificates approved by the tax administration. These digital certificates include the national ID number.

Question 9. Does the national electronic identity authentication service satisfy all the identity authentication needs for all your tax administration electronic services? If not, what tax services does it not support and why?

Denmark	The electronic identity certificate (digital signature) for the identity authentication service did not provide a service for certain taxpayers, including individuals under the age of 15 and foreign businesses who cannot obtain these certificates. The tax administration administers its own login service to its Internet services for these taxpayers.
Finland	We must enhance our identification service for foreign businesses and we must add two person identification features: - those people that are outside the Netbank identification need another solution and - person authorisation feature is lacking nowadays.
Korea	Our government provides public I- PIN (Internet Personal Identification Number) for national identity authentication, but we don't use public I-PIN for tax administration. We manage all tax information by national identity register number, however, public I-PIN provide only individual identity authentication for citizens, and public I-PIN doesn't provide national identity register number for citizens. So, we cannot use public I-PIN to provide taxpayer with tax information.
Norway	The national electronic identity authentication service did not adequately support authentication for foreigners and businesses.
Singapore	The national electronic identity authentication service provided no authentication service for companies and business.

Annex 2. Detailed responses to questions on private trusted third party identity authentication services

Question 1. Does your tax administration have a private trusted third party providing an identity authentication service? If yes, describe. What identity authentication and security issues have arisen?

Australia	Advised on the 'whole of government' service in operation in their jurisdiction, which provides a single key to access 'business to government' online services. They noted that credential registration and issuance were managed in-house by the tax administration, while a third party provided credential verification services. This third party provides two types of trust broker services: a Security Token Service supporting identity verification for clients using web services to interact with government and a User Authentication Service supporting login via an agency browser.
Denmark	Private trusted third party service provider is also used by the banking sector and the public sector, resulting in public concern regarding the extent of state knowledge of individuals' private affairs. They noted that the identity authentication service provider was regulated by the national IT and Telecom Agency.
Estonia	Banks provide the authentication service and no issues have arisen.
Finland	We use Bank Identification services for Person identification and we plan to use cell phones for that purpose as well. Identification prices may be high. Sometimes there are false identities but very seldom.
Japan	No issues have arisen in this area as only electronic certificates prepared by private certification authorities that have been verified as usable with the tax administration's online filing and payment systems are used.
Korea	We use the trusted third party identify authentication for identity authentication using digital certificate, mobile phone, credit card. Identity authentication using digital certificate is used for most of tax services. Identity authentication using mobile phone, credit card uses subscriber's information for identity authentication and is only used for taxpayer's family members to provide taxpayer with their information in "simplified year-end-settlement system".
New Zealand	The use of trusted organisations to process the authentication processes involved in the application for a tax reference number and noted isolated instances of false documentation having being supplied to obtain this number.
Sweden	Use an electronic identification document (e-ID) for user identification and to authorise a document or transmission. (The e-ID allows secure communication between companies, citizens and government agencies.) The e-ID is based on technology used in certain banks and by the leading telecom operator. These banks and the telecom operator provide trusted third party identity authentication services for the tax administration through the banks and the state post office.

Question 2. Are the identity proofs required the same as the identity proofs required for the national identity register? If no, describe the differences.

Korea	Typically, the third party use national identity register number for identity authentication. In the case of digital certificate, the third party register requires if individual, an application form, a copy of personal identification(national id-card, driver license, passport, etc) and signature, face-to face visit, if business, an application form, a copy of personal identification(national id-card, driver license, passport, etc) and signature of the person submitting an application and of representative, certificate of business registration, a copy of the authentication certificate of corporation's or representative's seal, face-to face visit. In the case of mobile phone and credit card, when taxpayers subscribe to mobile phone or credit card, they submit an application form, a copy of personal identification (national id-card, driver license, passport, etc) and signature, etc.
Spain	The identity proofs required by certification service providers as follows: the national ID card is required in the case of individuals and for businesses proof of the capacity of the person acting on behalf of the business is needed. (Note: In the National Context section Spain noted that the

	birth certificate was the required identity proof for individuals for the national register and that there was no national business register.)
Sweden	The same identity proofs are required by their certification service providers (including certain banks) and the national identity register, it may be of interest to readers to note that in order to become an online banking customer in Sweden, individuals must present in person at the bank and provide an identification document containing their national personal ID number.

Question 3. What identity information is held by the trusted third party?

Australia	Through the use of a strong authentication credential and by maintaining an audit trail of authentication events and user interactions.
Austria	Registration data;
Denmark	Private and public keys;
Finland	Person identification (name and TIN and certificates)
Japan	Personal details, such as full name, gender, date of birth, address, etc.
Korea	The third party register has their customer data (national identity register number, name, address, etc)
Sweden	The private trusted third party (banks and telecom operator) that manage the electronic identification document (e-ID) 'own' their customers, with government agencies paying for access to the data that is stored electronically on the e-ID instead of buying certificates.

Question 4. Does the trusted third party identity register interface with your tax administration? If yes, how does this operate?

Australia	Real time services are used to provide proof of identity from the tax administration's data to the third party during the registration processes.
Denmark	The tax administration requests the identity of the certificate owner from the third party when a taxpayer accesses their digital services and it uses certificates issued by the third party to employees in others areas of the public administration.
Estonia	The interface between the third party identity register and the tax administration involved the use of PIN codes.
Korea	In the case of digital certificate, the third party provide tax authority with the list of invalid digital certificate. When taxpayers try to request identity authentication, tax authority use that information to validate taxpayer's digital certificate. In the case of mobile phone and credit card, when taxpayer's family members try to request identity authentication, they provide tax administration with some information (subscriber's name and national identity register number, mobile phone number, credit card number, the valid period of credit card, etc). Tax administration sends that information to the third party and receives validity information.
Norway	The interface between the third party identity register and the tax administration involved APIs between the portal providing their eServices and the third party PKI provider.

Question 5. What are the benefits to your tax administration from having a trusted third party identity authentication system?

See general benefits described in paragraph 37 above. No other specific country benefits were reported.

Question 6. If you do not use a private third party identity authentication service, why not?

Belgium	Service not needed.
China	Legislation prohibited taxpayer information from being provided to third parties.

France & Ireland	No appropriate private third party identity authentication service exists;
Singapore	The tax administration manages the authentication process for identity numbers maintained by the tax administration. Authentication of the personal access PIN system (which is a common password used to transact between government agencies including the tax body) is at government level.
Turkey, Mexico & USA	Authentication was implemented by the administration itself.

Annex 3. Detailed responses to questions on identity authentication for internet services

Question 1. What systems or tokens do taxpayers use to access the Internet services?

Australia	We use the 'AUSkey' digital certificate to provide access to all business-to-government online services, for business (corporate and individual) taxpayers and tax intermediaries. They advised that it is planned to decommission the older digital certificate service currently used by the tax administration in 2012. They advised that the only service provided to employees is 'File a return', for which the token used is a share secret Authentication Solution (i.e. Tax reference number (Tax File Number) issued by the administration and password).
Belgium	Taxpayers access Internet service using an electronic ID card, containing the digital certificate, or Token and Username/Password.
Canada	User ID, Password and Shared Secrets system is used as identity authentication across taxpayer groups and between services.
Denmark	The authentication system in place is a digital certificate system, called *Nem*ID, with the taxpayer's private certificate key stored on a secure certificate server. The Taxpayer accesses the *Nem*ID certificate using a username, password and challenge code from a 'code-card'. The certificate server redirects the taxpayer to the relevant application server in the business/department requested.
Germany	Different tokens/ systems are in use for the services offered as follows: (i) a smartcard with Digital Certificate is used for the service to 'View tax account' information, (ii) a Digital Certificate softPSE or security stick or smart card is used to 'File a Return'.
Ireland	The system in place for an employee differs from that for business corporate/ business individuals and tax intermediaries. Three items are required of an employee accessing the tax administration's Internet services: the Personal Public Service Number (PPSN), a PIN and a shared secret question (one of three possible). The other customer groups use a Digital Certificate for accessing all services.
Japan	The tokens/ systems in place vary between services offered as follows: (i) User ID number and Password are used for accessing the following services: 'View tax account information', 'Amend taxpayer basic information' and to view confidential information sent by the tax administration; (ii) an electronic signature and electronic certificate are required in addition to user ID number and Password for the following services: 'File a return', 'Amend return details' and 'Claim repayments'; and (iii) details regarding the system used to access the service to 'Make a payment' are as follows: (1) Direct Payment Instruction via the online filing and payment system requires user ID number, Password, and a reference number for the tax payment. (2) A payment instruction for Internet banking requires login to the banking system, user ID number and Password. (Note: the requirements to login to the banking system are determined by each financial institution).
Mexico	A Digital Certificate is used for the service 'View tax account information'; User ID, Password and Digital Certificate are used for the other services provided, except in the case of Tax Intermediaries accessing the service to 'Amend basic information', which requires a token in addition to the User ID, Password and Digital Certificate.
New Zealand	In the case of viewing confidential information sent by the tax administration, the information is sent to a secure site for the customer to pick up after logging on; Make a payment involves referral to the customer's bank or intermediary to complete the transaction; all other services use a User code and Password. - Different tokens/ systems are used across taxpayer types and between services. In the case of business individual and employee taxpayer groups there are two elements to the authentication: i) a common authentication service for all public services (MinID), that uses a Password and physical PIN code sheet or SMS code; and ii) a private third party PKI service provider (Buypass) that uses a smartcard and PIN code. For the service 'Amend taxpayer basic' information, business corporate customers and tax intermediaries use the same token/ system as that used by business individuals and employees. However, for all other services, business corporate taxpayers and tax intermediaries use a two-factor authentication involving a Password and an SMS code.
Portugal	A User/ Password is used for business corporate taxpayer, while the three other taxpayer

	groups use either a User/ Password or Identity Token. (The User number is the same as the national ID number. The Identity Token consists of the national Citizen Card and ID number issued by the national authentication service.).
Spain	Differences in the tokens/ systems used across the three taxpayer groups and tax intermediaries, and in certain cases between services, as follows: business corporate taxpayers use a Digital Certificate; tax intermediaries use a Digital Certificate or Electronic National ID card; and employees use a Digital Certificate and Password. In the case of business individuals, the tokens/ systems used vary between services: (i) a digital certificate or an electronic national ID card or Tax ID number and tax records /reference number are used for the following services: 'View tax account information', 'File a return', 'Amend return details' and 'Amend taxpayer basic information'; (ii) a Digital Certificate and an electronic national ID card are used for the following services: 'Make a payment', 'Claim repayments' 'Submit bank account details' and to view confidential information sent by the tax administration.
South Africa	Use HTTPS Encrypted Active Directory supported by bespoke SQL Profile System. Sweden
Sweden	Security solution for all e-services is an electronic identification document (e-ID) that may be used as a smartcard or downloaded to the taxpayer's computer. They noted the following exception: where individuals agree to the pre-printed figures in their income tax return, a pre-printed code included in the tax return can be used to send in the approval via different media, (i.e. Internet, SMS, Telephone (Voice) and from 2011 by iPhone).
Turkey	Different tokens/ systems are used across taxpayer groups: business corporate customers and tax intermediaries use a User name and Password (which are provided by the local tax office); while information related to the motor vehicle licence is used in the case of business individuals and employees, whose access is limited to viewing information related to motor vehicle tax.
USA	A variety of tokens/ systems are used across taxpayer groups and services. An X509 Digital Certificate is required for 'File a return' and 'Amend return details', which are only available to business corporate taxpayers. Business corporate taxpayers, business individuals and employees are required to use a User ID, PIN and Password to access the service to 'Make a payment'. Business corporate customers also using an Electronic Federal Tax Payment System (EFTPS) for making federal tax payments. Regarding the service Submit bank account details, Business Individuals and Employees use the same token/ service, i.e. knowledge based Authentication Shared Secrets. Tax Intermediaries accessing the service to View client account information use e-services Registration User ID and Password.

Question 2. What identity proofs are required to register for Internet services?

Australia	Use Shared Secrets (e.g. name, date of birth, bank account details, etc.) as identity proofs for Employees accessing the service 'File a return'. The following identity proofs are required of the three other customer groups registering for the AUSkey Digital Certificate to access online services: the Australian Business Number (which is the single identifier for businesses) and name, date of birth and tax file number of a business associate (i.e. someone authorised to represent the business). In the case of AUSkey administrators: name, date of birth and tax file number are required.
Austria & Chile	Require a personal identification for the legal representative of the company, where relevant, in addition to other proofs e.g. in the former a Digital Certificate from an approved authority and in the latter tax records and a national ID number are required.
Canada	Registration process utilises a Two Factor Authentication (TFA) model (i.e. two independent means of evidence) as an additional security measure. The registration process utilises the TFA model by sending the tax administration security code by land mail (i.e. an out-of-band process). Identity proofing involves the provision of four shared secrets (i.e. social insurance number, date of birth, tax return information and postal/ ZIP code) and the creation of a user ID/password and security questions/ answers. A security code is posted to the address on record at the tax administration – this code is needed to access the online service. To complete the registration process, the user must login to the website within a specified period and enter the security code. Entering the security code is part of the original registration process. Future access to services is gained simply by entering the user ID and password. Different identity proofs are required by employees accessing 'File a return' (i.e. social insurance number, date of birth and access code from tax package). CRAs tax agent (tax intermediary) service (EFILE) authenticates using a number and password, which is provided to the tax agent after registration and screening. This number and password must match what is stored on the tax agent database otherwise the transaction is rejected. Business corporate, business individual

	and employees seeking to access the service 'Make a Payment' are transferred to a financial institution to complete that transaction.
Denmark	Corporate Business customers require a registration number from the business register (CVR system) to apply for a NemID[13].
France	Different identity proofs are required for different taxpayer groups. For identifying business corporate, business individuals and tax intermediaries the following proofs are required: (i) business national ID number; (ii) signed paper form (prefilled and to be printed from the website); and (iii) a signed mandate from the business legal representative (if applicable) authorising the employee (or intermediary agent) to access and use a list of e-services. In the case of Employees, the security of authentication is always based on three shared secrets: (i) the individual tax ID number: the administration noted that this is not really a secret, as it can be found on all the letters sent by the tax administration to the taxpayer; (ii) the personal 'e-services code': it is changed annually and can only be found on the prefilled income tax return (or a specific ad hoc letter in some cases); and (iii) the last tax reference income: it is an intermediary result of the PIT calculation and can only be found on the taxpayer's last PIT statement. The confidentiality of the last two secrets is based on the fact that they change annually and are only available on two different pieces of paper that are sent at two different periods of time in the year.
Germany	The identity proofs required differ across customer groups and between services offered and noted that due to a law for protecting tax-information, access to tax account-information is on a higher security level than to send data (file a return). Business Corporate and Tax Intermediaries: View tax account information: Registration for a tax portal is required with a tax number and shared secret (e.g. information from the last VAT return). A letter with registration information is then sent to the address saved with the tax number. This is needed to finish the registration. For Business Corporate taxpayer's registration must be done with a smart card. Access to account information requires an additional authorisation, e.g. in the case of Tax Intermediaries the client has to give a unique additional authorisation. File a Return: Similar to the method in place for View tax account information, registration for a tax portal is required with a tax number and a shared secret (e.g. information from the last VAT return). A letter with registration information is send to the address saved with the tax number. Confidential information sent by the tax administration: The taxpayer can only access the information by authenticating access with his/her certificate and only the taxpayer has the private encryption key to decode the data. Employees: View tax account information and File a Return: Registration for a tax portal is required with tax number and date of birth. A letter with registration information is send to the address saved to the tax number. In the case of View tax account information an additional authorisation is required to access account information. (Germany noted plans for registration without a letter: full-electronic registration with new electronic ID-Card-function.). Confidential information sent by the tax administration – the identity proofs required are the same as those for Business Corporate/ Tax Intermediaries.
Ireland	Business corporate, business individuals and tax intermediaries applying for a Digital Certificate must be previously registered with the tax administration. The Digital Certificate application process is a three-step process: between steps 1 and 2, and again between steps 2 and 3, a letter is issued via land mail to the address registered with the tax administration. Employees must provide a number of details as identity proofs (e.g. Personal Public Service Number, name, date of birth, mothers' birth surname, address, contact details), which are matched against the tax administration's records prior to issuing the PIN required for accessing online services.
Italy	The same identity proofs are required of business corporate and tax intermediaries, i.e. national ID Number, administrator corporate data, corporate data. The local administration office completes the registration process. Similarly, the proofs required of Business Individuals and Employees are the same, i.e. tax records and national ID number.
Japan	The identity proofs required are consistent across customer groups, but vary between services offered: (i) all services require a user ID and password; (ii) Certain services (i.e. 'File a return', 'Amend return' details, 'Claim repayments/ credits/ allowances' and 'Submit bank account details') require the use of a digital signature. Additional identity items are required in order to obtain an electronic certificate; (iii) the service 'Make a payment' (in addition to User ID and password) is governed by the provisions applying to Internet banking, which are determined by

[13] A NemID is a digital signature which can be used to log on to public services and Internet banking. The taxpayer's private key certificate is stored on a secure central server and the taxpayer accesses it using a username, password and code from a 'code card'.

	the relevant financial institution.
Mexico	Was one of only two respondents to report that they currently use biometrics (photo, ten fingers and iris), in addition to taxpayer ID, birth certificate and official ID. These identity proofs are required for all taxpayer groups and across all services offered. In addition to these proofs, a 'notarial patent' is required of Tax Intermediaries using the service Amend taxpayer basic information.
Norway	The same identity proof is required for Business Individuals and for Employees, i.e. *Min*ID (which is a common authorisation service for all public services). Registration to *Min*ID involves sending a physical PIN code sheet to the postal address recorded in the national identity register. This identity proof also applies to business corporate taxpayers and tax intermediaries accessing the service 'Amend taxpayer basic' information; for all other services accessed by these two customer groups the proofs required are as follows: Identification (SSN) of Chief Executive Officer (CEO)/ accountant is retrieved from national identity unit register. CEO's/ accountant's physical PIN code sheet sent to postal address recorded in the national identity person register.
Singapore	Different identity proofs required across customer groups. In relation to Business Corporate/ Individual customers, separate identity proofs are required for the business and the staff authorised to transact on behalf of the business: the Unique Entity Number (UEN) is required for identifying the business; authorised staff require a user ID (e.g. national ID number (IC number)/ Employment Pass number/ S Pass number/ Work permit number) and password (e.g. Singapore Personal Access Number* or PIN issued by the tax administration). The identity proofs required for Employees are the same as those required for identifying the staff authorised to transact on behalf of the business. In relation to Tax Intermediaries, the identity proofs required are as follows: for identifying the Tax Intermediary, the UEN; for identifying the Client (Business), the Client's UEN; for identifying the Client (Individual), the IC Number/ Employment Pass Number/ S Pass Number/ Work Permit Number; for identifying the Tax Agent Staff authorised to transact on behalf of the Client, User ID (e.g. IC Number / Employment Pass Number / S Pass Number / Work Permit Number) and Password (e.g. SingPass or IRAS PIN). *SingPass is used in conjunction with a national ID number to access e-services across government agencies.
Spain	Different identity proofs are required across taxpayer types: employees must use an internal user ID and the tax ID number; all other taxpayer groups require the tax identity number alone for identification.
Sweden	Access to online services is authenticated through the electronic identification document (e-ID) provided by the Swedish banking system. To apply for an e-ID an individual must present to the relevant bank in person and submit an identification document containing the national personal ID number. In the case of Employees accessing the service 'File a return', pre-printed codes are used: one to identify the user and the other one to authorise a document or transaction. The codes are pre-printed on the income tax return issued to the individual and can only be used once.
South Africa	Different identity proof requirements at the pre- and post-registration stages. Pre-registration requirements: Company Tax Reference number, IDs of individuals, Mandate/ Board Resolution and supporting documents as needed. Post-registration: User name and Password.
USA	Various identity proofs used by the administration, some of which were unique among survey responses: Business corporate: 'File a return': Registration process and suitability check. (Suitability is described as the process used by the US tax administration to determine if the firms or individuals listed on e-file applications and/ or Individual Taxpayer Identification Number (ITIN) applications are appropriate (i.e. suitable) to distribute electronic filing products and services under the administration's e-file. This may include an FBI criminal background check, credit history check, tax compliance check and prior history check for compliance in the administration's e-file.); ' Amend return details': Registration process includes a suitability criminal background check, fingerprint and credit check. 'Make a payment': EFTPS* enrolment process, Social Security Number (SSN) and Employer Identification Number (EIN)), name, address and bank account routing number. (*EFTPS – Electronic Federal Tax Payment System is a free service from the US to make federal tax payments online or by phone). Business Individuals and Employees; 'Submit bank account details: SSN, date of birth, ID number on the notice sent to the taxpayer by the administration.'Make a payment': the identity proofs are the same as those used for Business Corporate customers. Tax Intermediaries accessing 'View client tax account information' must provide a date of birth and SSN.

Question 3. How do you assure identity authentication and identity non-repudiation?

Ireland	Use digitally signed electronic envelopes that contain all the taxpayer's transaction information. These electronic envelopes are stored securely and can be retrieved if identity or transaction content is challenged and are accepted as legally sound documents.

Question 4. Why did you choose this token/system and authentication proof for this service?

Canada	The solutions chosen (shared secrets, user ID/ password, SSL encryption) were also an industry standard and cost effective.
Denmark	The system and the procedures in place were decided by The National IT and Telecom Agency in co-operation with the banking sector. This arrangement was selected because it was decided to use a common digital certificate (PKI) for both the public sector and the private sector. The main drivers for selecting the specific system were strong security and mobility. The private certificate is stored on a secure central server thus the user does not require any hardware to use the certificate. Access to the certificate is by username, password and a challenge code from a code card).
France	Originally digital certificate (PKI) was the only method available to all taxpayers and intermediaries accessing online services. However, ease of use became a greater priority to facilitate business taxpayers in fulfilling new legal obligations to file and pay electronically. An e-mail/password system was subsequently introduced for business corporate customers, The decision to implement access for employees, using shared secrets, was due to the fact that digital certificates were both expensive for the tax administration and complex to use for the taxpayer.
Ireland	Choice of a digital certificate for business corporate and business individual taxpayers is in line with national and EU legislation. They noted that their e-Commerce legislation, which is aligned with EU legislation, specifies that a digital signature using a digital certificate, where the private key remains under the sole control of the certificate holder, is admissible in evidence with the same weight as a written signature on paper. They noted that digital certificates are not used for authenticating employees as they did not offer the ease of use required by this taxpayer group. The system in place for providing employee identity authentication is based on personal data, a PIN, Personal Public Service Number (PPSN) and a secret question.
New Zealand	System was chosen for its multi user flexibility whereby a senior person in an organisation can allocate controlled access rights to staff.
Norway	The *Min*ID is a common authentication service for all public services. In relation to the other elements of their security system (e.g. use of password and SMS code for corporate business and tax intermediaries for most tax services), they noted that the authentication service is integrated in the portal
Sweden	The e-ID provides access to the online services via Internet banking, was an easy way to get 'identified' citizens, as the banks had already done the work. Most people in Sweden are regular e-banking customers and one of the reasons behind the successful level of participation is the non-complex secure way of accessing e-banking services over the Internet. The banking system provides the e-ID electronic identification document used for identification and authorising transactions. The PIN code system in place for approving income tax returns is considered very good for phone and mobile solutions. (Note: The e-ID was not in place when Sweden launched the first version of the income tax return on the Internet (2002) and thus an alternative system was introduced whereby customers could use a pre-printed figure in their return to send the approval by Internet, SMS, Telephone (Voice) and from 2011 by iPhone.)

Question 5 What are the main issues identified with the identity authentication systems in use and what solutions have been implemented or planned?

Issues regarding Digital Certificates	
Australia	Businesses experience difficulties applying for a digital certificate. The first certificate must be applied for, or authorised by a person senior enough to act on behalf of that business. Small

	businesses have a difficulty identifying the correct person and large businesses find it difficult to get a senior person to prioritise applying. The administration also reported issues in relation to browser compatibility. Issues are being addressed by simplifying the process and developing software enhancements.
Denmark	Private keys are stored on a secure central server which has been the cause of debates on privacy.
Mexico	Issues relating to service availability and forgotten keys. This is resolved by restoring service and the taxpayer obtaining a new digital certificate.
Spain	Taxpayers have found digital certificates troublesome e.g. the need to install the cert on a PC and the fact that the digital certificate has to be renewed periodically. We have addressed this by developing services that can be accessed using Revenue reference numbers and details while continuing to promote the use of the digital certificate and electronic national ID card.
Australia	Had a similar problem to Spain and addressed it through a user consultation process with clients. The new AUSkey digital certificate system aimed for a balance between usability and security. It was co-designed with clients and developers and leveraged learning from their earlier digital certificate system.
Sweden	Although the current model of e-ID is considered to have been relatively successful with many users, both in the public government that in the private sector, there are weaknesses. One is the lack of a coherent structure for the use of e-ID. Another problem is that today`s model is not open to potential new players to enter the market. In addition, today´s model is based on an old contract on e-ID. Although the solution existed for 10 years, there are still some users that think it is complicated to download the e-ID and to use it. The government has therefore established an e-ID Board, hosted by the Swedish tax agency to analyse issues.
Issues regarding Identity Authentication	
Denmark	Public sector and banking sector use the same identity authentication service. Taxpayers object to this, as they fear the State knowing too much about their private affairs.
Singapore	While there is a common identity authentication token for individuals, a SingPass, which can be used across government agencies no such token exists for business. A CorpPass is being explored to support business.
USA	The identity proofing process to allow tax agents to 'View Account information' can be cumbersome. The identity proofs required include date of birth, social security number, and power of attorney to act on behalf of a client and a password that must change every six months. Our new enterprise authentication solution would address this.
Issues regarding End-user Knowledge	
Belgium	Taxpayers are unfamiliar with the eServices available using their eID card. This should improve as more State services become available. Difficulties also relate to the maintenance and security of the browser support token and user name/password.
Canada	We use an 'Out of band activation code' in our secure access process and the associated letter that issues to taxpayers causes confusion. We are considering alternative options.
New Zealand	Online services are accessed using a user code and PIN. The application process is not fully electronic as the taxpayer must either go to a call centre or make phone contact to activate the registration. The solution proposes is to move to a government logon that can be used across a number of government agencies.

Annex 4. Detailed responses to questions on identity authentication for secure e-mail

Question 1. What systems or tokens do taxpayers use to access secure eMail services and what identity proofs are required to register for Secure eMail services?

Australia	A secure message option is available within the tax administration portals. This solution is not interfaced as an eMail to the clients desktop eMail system. The token/system used is the AUSkey digital certificate or the tax administration's PKI digital certificate. The following identity proofs are required of customers registering for the AUSkey Digital Certificate to access this service: the Australian Business Number (which is the single identifier for businesses) and name, date of birth and tax file number of a business associate (i.e. someone authorised to represent the business). In the case of AUSkey administrators: name, date of birth and tax file number are required.
Denmark	The token/system used for access to the secure eMail service is the *Nem*ID.[14] In relation to identity proofs, Denmark advised that corporate business customers require a registration number from the business register (CVR system) to apply for a *Nem*ID.
Finland	We have stated that this is not a service generally provided, but secure eMail is in use only with very exceptional cases where both agree to use it bilaterally.
Ireland	The tokens/ systems used to access the Secure eMail service vary across services and between customer groups: In general, a registered eMail address and password are required. In the case of business individuals accessing the service Amend taxpayer basic information a system-generated user password is sent by land mail to the registered address; the taxpayer must enter the password to decrypt information received. Tax intermediaries (agents) accessing the service Request client tax account information use a specific account number (Trader Access Account Number) issued by the tax administration (in addition to a registered eMail address and a password). The identity proofs required for this secure eMail channel were as follows: for identifying business corporate and business individual taxpayers, their tax reference number is used; for employees, the Personal Public Service Number (PPSN) is used; and for tax intermediaries, the Tax Advisor Identification Number (TAIN) is used for identification.
New Zealand	The token/system generally used for accessing services using Secure eMail is a user code and password. However, for business corporate taxpayers using the service Submit payment instruction the taxpayer transaction is initiated from their own bank/intermediary. In relation to the service confidential information sent by the tax administration, New Zealand advised that the information is sent to a secure site for the customer to access (after logging on).
Singapore	The token/system used for Secure Email is a User ID and password and outlined different identity proofs required across customer groups. In the case of business corporate and business individual taxpayers, separate identity proofs are required for the business and the staff authorised to transact on behalf of the business: the Unique Entity Number (UEN) is required for identifying the business; authorised staff require a user ID (e.g. national ID number (IC number)/Employment Pass number/S Pass number/Work permit number) and password (e.g. Singapore Personal Access Number (SingPass)[15] or PIN issued by the tax administration). The identity proofs required for employees are the same as those required for identifying the staff authorised to transact on behalf of the business. In relation to Tax Intermediaries the identity proofs required are as follows: for identifying the Tax Intermediary, the UEN; for identifying the Client (Business), the Client's UEN; for identifying the Client (Individual), the IC Number/Employment Pass Number/S Pass Number/Work Permit Number; for identifying the Tax Agent Staff authorised to transact on behalf of the Client, User ID (e.g. IC Number/Employment Pass Number/S Pass Number/Work Permit Number) and Password (e.g. SingPass or IRAS PIN).
Sweden	The tax administration provides an e-service (My messages) allowing taxpayers to have an account to receive simple messages from the authorities by eMail (and SMS). This first version only allows for one-way communication from the tax authority (the function will be further developed so that it also becomes possible to send messages to authorities). To obtain a business account at 'My messages' a person in the company is required to have sole signatory rights. The e-ID and taxpayer contact information are required to log into 'My messages'.

[14] A NemID is a digital signature that can be used for public services and Internet banking. The taxpayer's private key certificate is stored on a secure central server and the taxpayer accesses it using a username, password and code from a 'code card'

[15] *Sing*Pass is used in conjunction with a national ID number to access e-services across government agencies.

Annex 5. Detailed responses to questions on identity authentication for standard e-mail

Question 1. What systems or tokens do taxpayers use and what identity proofs are required to use Standard eMail services?

Belgium	The only service available through this channel is Request tax account information. Regarding the token/system in place, a Reference Number and an eMail address is posted to the taxpayer. They advised that low-level security is sufficient in this area as no critical information is provided using the standard eMail channel.
France	In the case of Business Corporate/ Individuals and Tax Intermediaries, only non-sensitive information is provided by e-mail in relation to the service Request tax account information. Where a detailed and potentially confidential reply is necessary, this is sent by post to the known postal address. In the case of employees using this and other services delivered by standard eMail ('Amend return details' and 'Amend taxpayer basic information') and where the information is sensitive, the following details are required from the customer: tax ID or full civil state (last name, first name, date and place of birth); full address; one piece of personal information from a pre-filled tax return or a tax statement.
Ireland	A token is not required for this channel. In relation to identity authentication, taxpayers (business corporate business individual and employees) are requested to include their Personal Public Service Number (PPSN) or their business number in all correspondence. Tax Intermediaries (agents) are requested to include their trader access identification number (TAIN), which is issued by the tax administration, and the client's PPSN or business number. Ireland noted that the risks associated with standard e-mail are clearly outlined to taxpayers and taxpayers are advised to use secure eMail for confidential communications.
Singapore	The token used for customers using standard e-mail to access services is the tax reference number. The identity proofs required of customers registering for this system are as follows: businesses must provide their Unique Entity Number; individuals must provide their personal ID number (e.g. IC number/Employment Pass Number/S Pass Number/Work Permit Number); and Tax Intermediaries provide the Unique Entity Number (business clients) or the ID number (individual clients).

Question 3. What issues have you identified and what solutions have you planned or implemented?

France	In the case of business corporate, business individual and tax intermediaries, only non-sensitive information is provided by standard eMail in relation to the service 'Request tax account information'. Where a detailed and potentially confidential reply is necessary, this is sent by post to the known postal address.
Ireland	Will accept all Standard eMails from taxpayers and tax intermediaries but will not send confidential information to a taxpayer or a tax intermediary using the Standard eMail channel. An alternative secure channel is used to respond.
New Zealand	Information is received from taxpayers by standard e-mail for most services available through this channel, but no taxpayer specific information is returned by standard eMail. In the case of business corporate customers, taxpayer specific information may be returned if a specific agreement is entered into. In relation to the service 'Confidential information' sent by the tax administration, the information is sent to a secure site for the customer to access (after logging on). The factors influencing the use of this system of authentication were ease of use/ implementation and security; appropriateness at the time when the service was introduced. Taxpayers are advised to use a B2B secure space e.g. Secure e-mail, instead of standard eMail.
South Africa	Taxpayers mainly use the standard eMail channel to submit supporting documentation requested by the administration.
Singapore	Confidential information is not sent to the taxpayer or intermediary by standard eMail. While taxpayers can make requests, any confidential information will be sent back to the taxpayer either via the online portal (which requires the taxpayer to authenticate himself/herself first),

	or through physical correspondences sent directly to his/her registered address.
USA	We do not provide services through standard e-mail in general, but outlined the following system in place for Tax Intermediaries: The Secure Object Repository (SOR) is an application designed to support requests for sensitive tax-related information. It provides a method to return sensitive, tax related information that cannot be sent using ordinary e-mail to register users. Each registered user has a Secure Object Repository where data is placed, or deposited. For most products, an e-mail is sent to the user alerting them data has been placed in their SOR. Depending on the type of data, and whether or not it has been read or left unread the system has timeframes to automatically delete the files. The token used is a username and password from e-services registration; the identity proofs required are date of birth, social security number, Adjusted Gross Income, etc.; these authentication methods were selected for ease of use and control.

Annex 6. Detailed responses to questions on identity authentication for telephone (voice)

Question 1. What systems or tokens do taxpayers use, why was this system or token selected and what identity proofs are required to use the Telephone (Voice) channel services?

Australia	The authentication process for this channel of communication involves a manual proof of identity (POI) conducted by the taxpayer service representative over the phone with the taxpayer or the taxpayer's intermediary. (The POI requirements are outlined in the Corporate Management Procedures and instructions.) The identity proofs required are an identifier (e.g. Tax File Number or Australian Business Number) and three data items held by the tax administration (e.g. letters or notices from the tax office). In the case of tax intermediaries just one data item is required, but their registration number and client identity information is also used. Australia advised that this authentication method was chosen in order to fulfil legislative requirements (i.e. Privacy Act and Commonwealth legislation), government policy and the tax administration's own policies and procedures.
Belgium	The identity authentication system in place for business individuals and employees, using the service 'Request tax account information', involves control questions asked by the tax administration of callers. The identity proofs required are personal company data (including Enterprise number) or personal data (including national number). This authentication method was chosen for simplicity.
Canada	The following describes the authentication process for individuals and businesses seeking account specific information over the telephone: The process involves a manual proof of identity conducted by the telephone agent over the telephone with the taxpayer. The identity proofs required for individuals are a social insurance number, full name and address to be verified against name and address on record, and date of birth. In addition the taxpayer must answer two additional questions based on other account information available, e.g. Names and dates of birth of children. The identity proofs required for businesses are the business name, business number, business address, the owner or director's name, and their social insurance number if applicable. In addition the caller must answer at least two additional account specific questions.
France	In the case of business corporate, business individuals and tax intermediaries, only non-sensitive information is provided via this channel of communication in relation to the service Request tax account information. Where a detailed and potentially confidential reply is necessary, this is sent by post to the known postal address. In the case of employees using this service and where the information is sensitive, the following details are required from the taxpayer: tax ID or full civil state (last name, first name, date and place of birth); full address; one piece of personal information from a pre-filled tax return or a tax statement.
Germany	The identity authentication system in place for all customers accessing the service Request/ View tax account information involves checking identity via phone number/ recall or shared secret (e.g. VAT number).
Ireland	All taxpayers and tax intermediaries who access services by the telephone (voice) channel must be registered with the tax administration and tax intermediaries must also be linked to their own taxpayer clients with the tax administration. Irish taxpayers are required to confirm at least two items of data held on the Irish tax administration's system, for example, sources of income, name, address of their tax intermediary, date of birth, name of previous employer, details of existing tax allowances, mother's pre-marriage name, date of commencement/cessation of work, name of previous employer. In cases of any doubt, the information will be provided either through a telephone recall (using contact details on record or available independently) or by post to the address on the administration's system. Irish tax intermediaries must confirm two items of data on record regarding the taxpayer that the intermediary would be expected to know. In cases of any doubt, the caller is not provided with the information and instead the details are posted directly to the taxpayer.
New Zealand	The token or system used to authenticate the identity of taxpayers accessing services by the telephone (voice) channel is a validation process involving a series of questions to ensure the caller is authorised. In relation to identity proofs, this information is referenced against details on file and the unique identifier (IRD number issued by the tax administration). This process was selected because it satisfied the requirement to uphold the integrity of the tax system,

	whilst being relatively easy to use.
Singapore	The token or system used is the tax reference number. The identity proofs for different taxpayer groups are as follows: businesses use their Unique Entity Number; individuals use their IC Number/Employment Pass Number/S Pass Number/Work Permit Number; and tax intermediaries use a Unique Entity Number (business clients) or an Identity Number (individual clients). Singapore advised that when confidential information is requested, this information is sent to the taxpayer either via the online portal (which requires the taxpayer to authenticate him/herself first), or through physical correspondences sent directly to his/her registered address, or over the phone only when the identity of the company director can be established (i.e. the company director must make the phone call).
Spain	The tokens or systems used are the fiscal ID number and a reference number. Various identity proofs may be required to access services via this channel, i.e. the fiscal ID number and revenue records or the electronic national ID card. They noted that the authentication method was selected in order to facilitate ease of access to basic services.
Sweden	The security solution for all e-services is an electronic identification document (e-ID) that may be used as a smartcard or downloaded to the taxpayer's computer or mobile phone. Note the following exception: where individuals agree to the pre-printed figures in their income tax return, a pre-printed code included in the tax return can be used to send in the approval via different media, (i.e. Internet, SMS, Telephone (Voice) and from 2011 by iPhone).
USA	Our system of authentication involves a verbal exchange using information such as tax ID, Social Security Number (SSN), Employer ID number (EIN), Individual Taxpayer ID number (ITIN), name, address, filing status, date of birth. Registration is not required. If a taxpayer has received a notice, it will contain a PIN, which can be matched with the SSN or EIN. This authentication method was selected for ease of use.

Annex 7. Detailed responses to questions on identity authentication for telephone (SMS)

Question 1. What systems or tokens do taxpayers use, why was this system or token selected and what identity proofs are required to use the telephone (SMS) channel services?

Australia	We do not accept any inbound messages by telephone (SMS); therefore no authentication process is required. They advised that they provide an alert and a reminder service only by telephone (SMS).
Chile	The following authentication process in place for business corporate, business individual and employee taxpayers accessing the service 'File a Return' by telephone (SMS): the tokens/systems used are ID/password and/or Digital Certificate; the identity proofs required are the national ID number, tax records and/ or personal data. The authentication method was chosen for security and ease of use.
Ireland	The token/system and identity proofs required of taxpayers accessing services by telephone (SMS) are the Personal Public Service Number (PPSN) and PIN (issued by the tax administration). For example, both the PPSN and PIN are required in order to use the service 'Claim a tax credit'. Confidential information is not issued by telephone (SMS), instead it is posted to the taxpayer registered address. Employees must provide the following identity proofs to apply for a PIN; a PPSN, name, date of birth, mothers' birth surname, address and contact details. These details are cross referenced against the tax administration's records prior to issuing the PIN. Amendments by telephone (SMS) to the taxpayer name and/ or address are manually screened by the tax administration. The authentication method was selected for ease of use and strength of security. The mobile telephone number used to submit the changes is recorded and retained by the administration.
Spain	The tokens/ systems used to file a return are the Fiscal ID number and reference number; while for the service Request/ View tax account information, fiscal ID number and revenue records are required. The identity proofs used are as follows: national ID number/ Fiscal ID number and revenue records, or Digital Certificate, or electronic national ID card. This authentication system was selected in order to facilitate access to basic services using a device belonging to the taxpayer.
Singapore	An authentication process is not required as telephone (SMS) is used only for broadcasting generic messages to taxpayers or for the receipt of simple enquiry services that do not require any authentication. While taxpayers can make requests, confidential information is not provided by telephone (SMS), but instead is sent to the taxpayer either by use of the online portal or by post to the registered address.
Turkey	Taxpayers could view information related to motor-vehicle tax using motor-vehicle licence information for authentication. This authentication system was selected for ease of implementation.

Annex 8. Detailed responses to questions on identity authentication for telephone IVR (Interactive Voice Response)

Question 1. What systems or tokens do taxpayers use, why was this system or token selected and what identity proofs are required to use the telephone (IVR) channel services?

Australia	Authentication methods were chosen for ease of use and security reasons (e.g. the specific identifiers are known only to the customer and the tax administration, voice is recorded and a recorded declaration is a virtual signature). The transactions related to the services 'Request tax account information' and 'Make a payment' are considered low risk. Details in relation to the authentication measures for various services are as follows: 'Request tax account information': The identity proof required is the Tax File Number (TFN), which is entered into the phone via a touch-tone service. No tax account information is provided, only a progress report of refund activity. 'File a return': The customer enters proof of identity information into the phone via the touch-tone service. The following identity proofs are required: TFN, Australian Business Number, Document ID Number issued by the tax administration, and a binding recorded declaration. (Sole traders are required to provide date of birth and postcode). 'Make a payment': IVR lodgements and payment arrangements for debt pilot are through speech recognition. The identity proofs required are as follows: for Activity statement payments, data required is an ABN and debt amount within 10% accuracy. For Income tax account payments, data required is TFN and debt amount within 10% accuracy. The identity proofs required of Employees using the IVR facility to make a payment arrangement are the TFN and debt amount within 10% accuracy. The customer can enter the numeric numbers via speech recognition. 'Claim repayments, credits, allowances': the tokens/ system involved are fuel tax credits registration, ABN, EIN and DIN and declaration. The identity proofs required are the ABN, Document ID number, EIN, a binding recorded declaration, and tax practitioner identifier, where relevant. In the case of Employees the identity proofs required are the TFN, date of birth, postcode and binding recorded declaration. The customer can enter the numeric numbers into the touch-tone phone.
Canada	Authentication system in place for employees accessing the service 'File a return' as follows: the tokens/ systems used are ID proofing information, personalised access code and shared secret validation. The factors influencing the choice of this system of authentication were the balance between security and user experience, as well as cost effectiveness.
Chile	The following authentication system for business corporate and business individual taxpayers accessing the service 'File a return' via this channel: the tokens/ systems used are an ID/password and/or Digital Certificate; while the identity proofs required are the national ID number and revenue records and/or personal data. This system of authentication was chosen for strength of security and ease of use.
Ireland	The authentication system in place for different taxpayer groups and services. In the case of business corporate and business individual taxpayers accessing the service 'Request tax account information' the tax number is used to order a Statement of Account, which is sent to the address on file for that business. Regarding Employees, the token/ identity proof required to access services is the taxpayer's Personal Public Service Number (PPSN) and also a PIN in certain cases. For instance, the taxpayer's PPSN is used to access the service 'Request tax account information'. However, both a PPSN and PIN are required to authenticate taxpayers using the services 'Amend taxpayer basic information' and 'Claim repayments, credits and allowances': The factors influencing these methods of authentication were ease of use and security. In general, minimal authentication is required as information is not provided over the telephone, but instead is sent to the postal address on the tax administration's records.
New Zealand	Our authentication system, which varies across customer groups and between different services, but is generally based on the use of an IRD number (which is a unique number issued by the tax administration) and PIN. The system was chosen for ease of customer use. The details in relation to various services are as follows: 'Amend taxpayer basic information': customers using this service to notify a change of address are required to enter their IRD number. In the case of Tax Intermediaries, the client's IRD number, a PIN and the tax agent number are required. Only Tax Intermediaries require an identity proof to access this service, namely a PIN. 'File a return': This service only applies to Employees in relation to the Personal Tax Summary* and access to it requires the customer's IRD number and confirmation of address details. (*A Personal Tax Summary is an assessment for salary/ wage earners calculated by the tax administration). 'Request tax account information': certain limited

	information can be requested through this service by entering the IRD number, while a PIN is required to access confidential information.
Singapore	While taxpayers can make requests for information via this channel, confidential information is not provided via IVR, but instead is sent to the taxpayer either via the online portal or by post to the registered address. The token/ system used is the tax reference number and the identity proofs required are as follows: businesses use the Unique Entity Number; Individuals use personal ID numbers (e.g. IC number/Employment Pass Number/S Pass Number/Work Permit Number); and Tax Intermediaries use the Unique Entity Number (business clients) or ID number (individual clients).
Spain	The tokens/ systems used to access services via this channel of communication are the fiscal ID number and revenue records. In the case of business individuals accessing the service Request tax account information the national ID and revenue records are required. The identity proofs used for all customer groups/ services are as follows: national ID number/ fiscal ID number and revenue records or Digital Certificate or electronic national ID card. This authentication system was selected in order to facilitate access to basic services using a device belonging to the taxpayer.
USA	We provide an IVR facility for business individuals accessing certain services (i.e. 'Request tax account information', 'Make a payment' and 'Submit bank account details'). The administration advised that only basic information can be accessed via touch-tone. It is mainly used to route the customer to the appropriate customer service representative to be authenticated with verbal exchange questions. Ease of use was noted as the reason for choosing the authentication system in place, the details of which are outlined below for individual services: 'Request tax account information': the token/ system used are the Social Security Number (SSN), Employer ID number (EIN), Individual Taxpayer ID number (ITIN) and the tax year. In relation to identity proofs, the administration advised that registration is not required. If the taxpayer receives a notice, a PIN will be included. The SSN or EIN is matched with the PIN. 'Make a payment': the token/ system used to access this IVR option is EIN/ SSN and PIN. The identity proofs required for enrolment to use this service are the SSN/ EIN, PIN and Bank Routing Number. 'Submit bank account details': the token/ system used is knowledge based authentication/ shared secrets. The identity proofs required are the SSN, date of birth and PIN

Question 2. How do you assure identity authentication and non-repudiation?

Australia, Canada, Ireland, Chile & USA	Validate control questions against their administrations record.
Australia	All calls are recorded.
Ireland	Records calls and advised that information issued was sent by land mail to the address on record. Requests to amend customer name and address were redirected to a person and dealt with manually.
New Zealand	Do not employ any measures to satisfy non-repudiation.
Singapore & USA	Measures are not required as no confidential information is provided.

Question 3. What issues have you identified and what solutions have you planned or implemented?

Australia	One of the identity proofs required in order to make an Income tax payment using IVR is that the taxpayer/agent must enter the debt amount within 10% accuracy which they feel is not as reliable as they would like. They also report that they can't provide account information via this channel. We plan to implement a more stringent and automated proof of identity system which should provide a solution to these issues.
New Zealand	No identity authentication is performed. It is proposed to introduce identity authentication measures.