OECD FORUM ON TAX ADMINISTRATION

Tax Administration 3.0 and the Digital Identification of Taxpayers

Initial Findings

OECD
BETTER POLICIES FOR BETTER LIVES

OECD Forum on Tax Administration

Tax Administration 3.0 and the Digital Identification of Taxpayers

Initial Findings

This document, as well as any data and any map included herein, are without prejudice to the status of or sovereignty over any territory, to the delimitation of international frontiers and boundaries and to the name of any territory, city or area.

This document was approved by the Committee on Fiscal Affairs on 13 September 2022 and prepared for publication by the OECD Secretariat.

Please cite this publication as:
OECD (2022), *Tax Administration 3.0 and the Digital Identification of Taxpayers: Initial Findings*, OECD Forum on Tax Administration, OECD, Paris, https://doi.org/10.1787/3ab1789a-en.

Photo credits: © Shutterstock.com, Gettyimage.com, Istockphoto.com, Alex Butterfield (cc-by-2.0), Unsplash.com

Preface

I am pleased to present this report about digital identity and tax. Secure identification of taxpayers is key to the efficient functioning and matching of administrative processes in modern tax administration, helping to create new opportunities for tax administrations across the world to help citizens pay the right tax at the right time. At the same time advances in technology are also facilitating the building-in of some taxation processes into the systems that taxpayers use to complete transactions, run their businesses and communicate with each other. This in turn has the potential to unlock further significant reductions in compliance burdens and tax gaps, and is the vision of Tax Administration 3.0.

A key part of achieving this vision is the creation of effective digital identity systems which can support the greater linking of public and private systems in an ever more digital and global society, including across borders. As part of the ongoing work to support tax administrations in their journey to Tax Administration 3.0, this report explores two aspects of digital identity relating to tax.

Firstly, it provides experiences from countries around the world on how the development of digital identity has been intertwined with the journey of digitalisation of tax in a domestic setting. This will hopefully be helpful to countries that have more recently embarked on the journey of digital transformation or whose countries are considering the introduction of digital identities, whether government wide or for tax purposes.

Secondly, the report seeks to explain some of the cross-border challenges connected to digital identity and tax. A selection of cross-border situations with implications related to service levels, burdens, and tax compliance, both in the home and host country, were identified as areas where cross-border digital identity solutions might be of particular benefit. This is something that is being looked at in concrete form in the 2022 OECD report *Tax Administration 3.0 and Connecting with Natural Systems: Initial findings*. Taken together, these two reports will hopefully stimulate further work and international cooperation in this area, as well as give weight to tax issues in the consideration of domestic priorities and strategic developments relating to digital identity.

Finally, I would personally like to thank all of the tax administrations which formed the Advisory and Drafting Group - Australia, Canada, Finland, Indonesia, Spain and the United States - for their high quality inputs into this report, as well as the FTA Secretariat for their support. As members of the FTA community, we are all on our unique digital transformation journeys, given inherently different starting points, histories, experiences, systems, and objectives. There are still, though, many similarities in the challenges we face which can often be informed, or indeed addressed through close international cooperation.

Nina Schanke Funnemark,

Commissioner of the Norwegian Tax Administration

Nina Schanke Funnemark

Foreword

The *Tax Administration 3.0: The Digital Transformation of Tax Administration* 2020 ("Tax Administration 3.0") report identified digital identity as one of core building blocks for enabling future seamless tax administration, facilitating the building-in of taxation processes into the interconnected natural systems that taxpayers use to transact, run their businesses and communicate. This in turn has the potential to unlock further significant reductions in compliance burdens and tax gaps. One of the primary actions taken forward after the publication of the report was to explore the current state of play on digital identity, the different domestic solutions adopted in a number of jurisdictions as well as the challenges related to cross-border taxation processes. The intention was to lay the ground for future collaborative work in this area, including with business and other stakeholders.

The work was led by an Advisory and Drafting Group (ADG) consisting of tax administration officials from Australia, Canada, Finland, Indonesia, Spain, Norway (Chair) and the United States, supported by the FTA Secretariat. This focussed on two activities:

- Knowledge sharing on business cases, strategies and legal frameworks adopted by different tax administrations (which may be at the tax administration or government level). The intention is to help inform tax administrations in developing their own approaches to the establishment and use of digital identities.
- Understanding where international digital identity solutions might be desirable to support the identification of taxpayers in cross-border situations, for example in supporting service delivery to non-resident taxpayers and identifying taxpayers and liabilities related to global platform-based business models.

In addition to reviewing what could only be a small part of the extensive literature on digital identity, the project group made particular use of several specific data collection efforts. These were:

- The Inventory of Tax Technology Initiatives (ITTI) which contains information on technology tools and digitalisation solutions implemented by 80 tax administrations. The inventory data is collected through a global survey on digitalisation which contains a section on digital identity.
- The Digital Transformation Maturity Model, now completed by over fifty jurisdictions.
- ADG-member country case studies of domestic digital identity implementation, presented in Annex A.
- ADG-member country specific explorations of taxpayer identification challenges in cross-border situations, in Annex B.

Acknowledgements

This document was authored by Rex Arendsen from the FTA Secretariat, with input and assistance from Peter Green, Raffaele Articolo, Sonia Nicolas, José Puig Pimentel and the Communications Team of the OECD Centre for Tax Policy and Administration. The author would also like to thank Cecilia Emilsson and Barbara Ubaldi both from the OECD's Open and Innovative Government Division, for reviewing the report and for their valuable comments. A particular thanks goes to Line Wilberg and Mariken Holter from the Norwegian Tax Administration for chairing the project's Advisory and Drafting Group and to Marianne Henriksen and Dag Helge Gundersen from the Norwegian Tax Administration for co-creating the descriptions and analysis of taxpayer identification challenges in Annex B.

The author would like to thank the members of the Advisory and Drafting Group for their guidance and valuable contributions, in particular: Carmel Rugolino, Elissa Walker and Percy Lara from the Australian Taxation Office; Ron Droeske, Brian Rae and Johnathan Wasylycia from the Canada Revenue Agency; Milja Kiviranta and Pasi Sinervo from the Finish Tax Administration; Nidya Hapsari, Leli Listianawati, Satrio Adhi Wibowo, Agung Wibowo and Achmad Ginanjar from Indonesia Directorate General of Taxes; Marianne Henriksen, Mariken Holter and Dag Helge Gundersen from the Norwegian Tax Administration; Carlos Marcos from the Spanish Tax Agency and Theresa Franzke, Erick Bell and Frank Guida from the United States Internal Revenue Service.

Table of contents

FIGURES

TABLES

Abbreviations and acronyms

AEAT	Agencia Estatal de Administración Tributaria (Spanish Tax Agency)
ATO	Australian Taxation Office
CIT	Corporate Income tax
CMS	Credential Management Service
CRA	Canadian Revenue Agency
CSP	Credential Service Providers
DGT	Directorate General of Taxes (Indonesia)
DNI	National Identity Document (Spain)
EFIN	Electronic Filing Identification Number
eIDAS	electronic Identification, Authentication and Trust Services
FTA	Forum on Tax Administration
GST	Goods and Services Tax
HST	Harmonised Sales Tax
ID	(digital) Identity
IDP	Identity Provider
IRCC	Immigration and Citizenship Canada
IRS	Internal Revenue Service
ITTI	Inventory of Tax Technology Initiatives
MSCA	My Service Canada Account
NIK	National Identification Number (Indonesia)
NIST	National Institute of Standards and Technology
NPWP	Permanent Taxpayer Identification Number (Indonesia)
PAYE	Pay As You Earn
PCTF	Pan-Canadian Trust Framework
RAC	Represent a Client
RAM	Relationship Authorisation Manager
SME	Small and Medium Scale Enterprise

TDIF	Trusted Digital Identity Framework
TDIS	Trusted Digital Identity System
TIN	Tax Identification Number
VAT	Value-added tax

Executive Summary

This report represents a first step in exploring the current state of maturity of the use of digital identities within tax administrations, both domestically and across borders, taking advantage of the results of the Digital Transformation Maturity Model and responses to the survey underpinning the new Inventory on Tax Technology Initiatives. This report has been undertaken in the context of possible further work within the Forum on Tax Administration (FTA) both on continued knowledge sharing in this area and on the development of potential collaborative solutions to cross-border use cases.

Digital identity is one of the core building blocks of future tax administration as envisioned in the Tax Administration 3.0 report. Effective digital identity management is a prerequisite for the greater linking of public and private systems with taxpayers' natural systems to enable the trusted remote connections required for seamless taxation.

As shown in Chapter 1 of this report, many tax administrations have or are in the process of adopting the more secure and sophisticated digital identity systems needed to allow access to an increasing range of taxpayer services, including for registration, personal and business data management, tax declarations and payments. Digital identity is also increasingly being used domestically to join-up government services and, in some countries, to allow a wider range of connections with private sector services. The attributes and credentials used to create secure digital identities can now also reflect multiple different personal and official processes, as well as different roles, for example as an individual taxpayer, business or taxpayer representative. The report supplements this overview with a set of detailed case studies drawn up by the administrations which led the work on this report.

Progress on the creation of digital identities which can be used across borders has been slower, although significant advances have been made in regional frameworks, such as within the European Union. While over time developments in digital identity frameworks might allow for greater global interoperability, in the meantime the lack of acceptance of domestic digital identities across tax administrations globally can lead to continuing frictions and costs and as well as presenting compliance risks. In this global context:

- Taxpayers are often confronted with paper processes and multiple identity systems. In many cases it may not be easy to comply with requirements, and they may have to initiate and orchestrate cross-border tax administration processes themselves.
- Third parties are being challenged with different sets of data collection and reporting obligations and standards. A key challenge is to ascertain the tax status of their international counterparties, which is especially challenging where there are high volumes of transactions.
- Tax administrations in some cases struggle to engage with the right taxpayer at the right moment, causing risks of double or non-taxation. In addition, paper processes affecting multiple internal departments can cause major administrative burdens and inefficiencies.

These challenges are already significant and are likely to grow along with the digitalisation of the global economy and the increased ability of individuals and businesses to operate across borders.

Chapter 2 therefore analyses some of the issues facing individuals and businesses in a cross-border context, including through the presentation of a number of use cases as identified by the participating tax administrations in Annex B. Chapter 2 also briefly presents the possible further work that might be undertaken following the publication of the 2022 OECD report *Tax Administration 3.0 and Connecting with Natural Systems: Initial findings* (OECD, 2022[1]) which might lead to the development of a framework allowing domestic digital identities to be used in specific areas of cross-border taxation. In addition, it would be useful to work with taxpayer representatives globally on the further identification and quantification of areas where a lack of digital identity interoperatibility is causing significant issues.

Caveat

Tax administrations operate in varied environments, and the way in which they each administer their taxation system differs with respect to policy and legislative environments as well as administrative practices and cultures. A standard approach to tax administration may be neither practical nor desirable in a particular instance. Therefore, this report and the observations it makes need to be interpreted with this in mind. Care should be taken when considering a tax administration’s distinct practices to fully appreciate the complex factors that have shaped a particular approach. Similarly, regard needs to be had to the distinct challenges and priorities each administration is managing.

References

OECD (2022), *Tax Administration 3.0 and Connecting with Natural Systems: Initial findings*, OECD Publishing, Paris, https://www.oecd.org/tax/forum-on-tax-administration/publications-and-products/. [2]

1 Domestic Digital Identities

Introduction

The secure identification of taxpayers is key to the efficient functioning of modern tax administrations allowing the matching of administration processes (communication, tax return filing, incorporation of other data sources, self-service options, etc.) to individual and business taxpayers.

To facilitate the identification of individuals and businesses that are, or may be, subject to tax obligations, tax administrations have long used registration and identity verification processes to create taxpayer registers. To ensure the accuracy of the registers and to streamline internal processes across the administration, in particular matching data to taxpayers, administrations have issued individual taxpayers with tax identification numbers (TINs) or equivalent unique identifiers.

As paper-based taxation processes gave way to the digitalisation of tax administrations, these identifiers became integrated into digital identities. These digital identities are an electronic representation of an individual or business which enables them to be distinguished when interacting online, such as when filing a tax return or making an online payment. It also enables taxpayers' information to be joined-up more effectively in electronic processing within the administration, both for compliance purposes and to provide better services.

Over time these have become more secure as administrations start to develop a range of self-service options, including the ability for taxpayers to change their personal information, view their tax positions or request refunds. Digital identities now often include a wide range of attributes which allow for more secure authentication processes and the granting of a wider range of permissions. The digital identity system composes two parts:

- digital attributes of the taxpayer such as name and address, date of birth, residency, taxpayer status or statuses and potentially many other attributes; and
- the authentication of the taxpayer seeking to use digital identity through checking against aspects of the digital representation.

Of course, digital identities provide far wider opportunities than just for tax administration. Over the years, each country has developed its own digital ID infrastructure, often composed of a patchwork of domain specific identity systems. Increasingly governmental organisations have been focussing on digital service delivery to its residents and the enhancement of service quality. As envisaged in Tax Administration 3.0, this is also a necessary part of achieving the goal of seamless tax administration, allowing the further driving down of tax gaps and compliance burdens. The essence of that vision is that tax administration processes are increasing built into taxpayers' natural systems which, in turn, are increasingly connected with other public and private sector systems, all reliant on secure digital identity.

This chapter focuses on the current state of play regarding digital identity within tax administrations and also looks briefly at some aspects of interoperability. Chapter 2 will look at cross-border interoperability issues and developments, as well potential interoperability solutions which may be able to be applied for specific taxation processes. (Some definitions of aspects of digital identity in the context of this paper are in the glossary section.)

Digital identity maturity in tax administrations

Tax administrations can, and have played different roles with respect to the implementation of Digital Identities for citizens and businesses in different jurisdictions, for example as regards:

- the *enrolment and provision of digital identities*, based on the administration's network of physical offices and contact points and the availability of taxpayer identifying data in registries. In some countries, the tax administration has also been central in driving the uptake and adoption of digital identities by citizens and businesses, whether as a 'launching platform' or via targeted mandating strategies;
- the *provision of credentials*, in many cases related to being one of the first large governmental organisations using digital identities, including in combination with specific risk mitigating measures;
- *unlocking taxpayer services* via the use of digital identities, which can make a tax administration a key partner within the wider domestic digital identity landscape, as well as a major user of digital identity services, including those developed by other parts of government and the private sector.

These roles and responsibilities can of course vary over time, triggered by developments such as a maturing national digital government infrastructure, the availability of whole-of-society solutions or business case adaptations. Of course, each tax administration operates within a specific domestic context in which each role brings about specific responsibilities and governance arrangements.

The Forum on Tax Administration (FTA) Digital Transformation Maturity Model

The FTA Digital Transformation Maturity Model (OECD, 2022[2]) was developed in order to provide tax administrations globally with a tool to allow them to self-assess their current level of maturity against the building blocks identified in Tax Administration 3.0 and to facilitate consideration of future strategy. The Digital Identity building block section of the Model, which is split into two sections – the creation and use of digital identity - is reproduced at Annex D while the overview of the results can be found in Chapter 2 of the Digital Transformation Maturity Model report (OECD, 2022[2]).

The Digital Identity path of growth presented in the Maturity Model can be characterised as:

- moving from tax administration specific and less secure identification methods to highly personalised and information rich digital identities which can be used for secure processes across government, and eventually, the whole of society;
- progressing from the development of taxpayer centred processes like filing and reporting towards a connected ecosystem approach bringing together different parts of government and the private sector;
- enhanced interoperability between solutions and solution providers supporting the secure and unique identification of taxpayers and citizens in a joined-up way, helping to reduce burdens and helping to move taxation processes into the background.

The Maturity Model sets out five levels of maturity from Progressing to Aspirational. The middle level – Established – was designed to represent where most well digitalised tax administrations are currently. The Aspirational level represents the future tax administration model envisioned in Tax Administration 3.0.

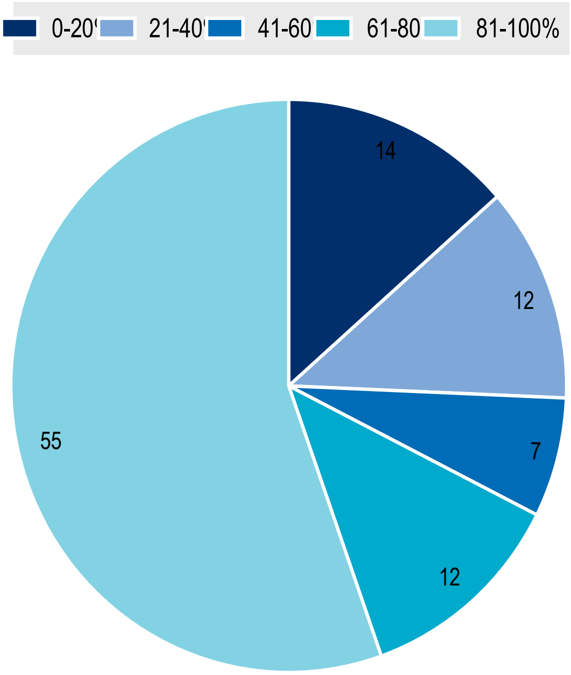
Currently, as expected, the majority of tax administrations assess their digital identity maturity level as being established (OECD, 2022[2]).

Acceptance by taxpayers

The widespread take up and acceptance of digital identities by both individual and business taxpayers is critical, and the launch of the Inventory of Tax Technology Initiatives, underpinned by a survey based on the Tax Administration 3.0 building blocks, has provided more detailed evidence on the uptake and use cases for digital identity.

Overall, tax administrations report high adoption rates of digital identities for private and business taxpayers accessing digital tax administration services. Nearly 55% of participating tax administrations responded that in their jurisdiction more than 80% of individual taxpayers use a digital identity, (see Figure 1.1). On the other hand, 26% of the tax administrations still indicate that in their jurisdiction 40% or less of individual taxpayers use a digital identity to engage with the tax administration.

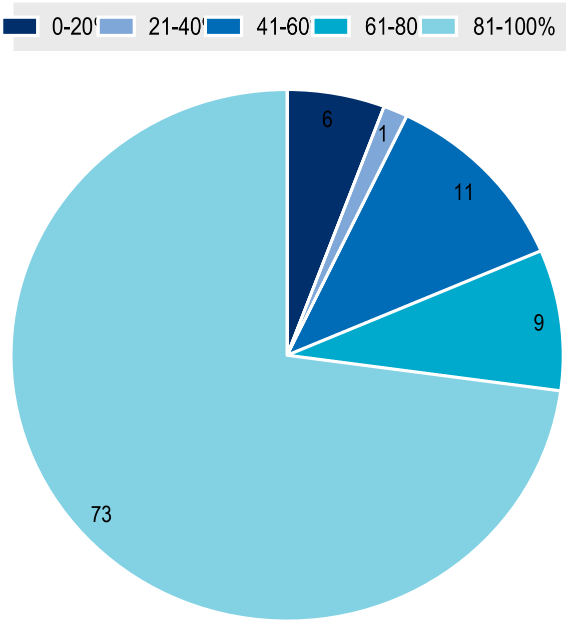
Figure 1.1. Percent of administrations estimating the take-up rates of individual taxpayers using digital identities



Note: This figure summarises the responses to the question in the global survey on digitalisation: “Of your individual taxpayer population, please indicate the estimated percentage that use an approved digital identity to access secure digital services offered by your administration”.
Source: OECD et al. (2022), Inventory of Tax Technology Initiatives, https://www.oecd.org/tax/forum-on-tax-administration/tax-technology-tools-and-digital-solutions/, Table DI1 (accessed on 3 August 2022).

Regarding the population of business taxpayers, adoption rates are higher. Nearly 75% of participating tax administrations responded that in their jurisdiction more than 80% of business taxpayer use a digital identity, see Figure 1.2. Only 7% of the tax administrations indicated that in their jurisdiction less than 40% of business taxpayer use a digital identity.

Figure 1.2. Percent of administrations estimating the take-up rates of business taxpayers using digital identities



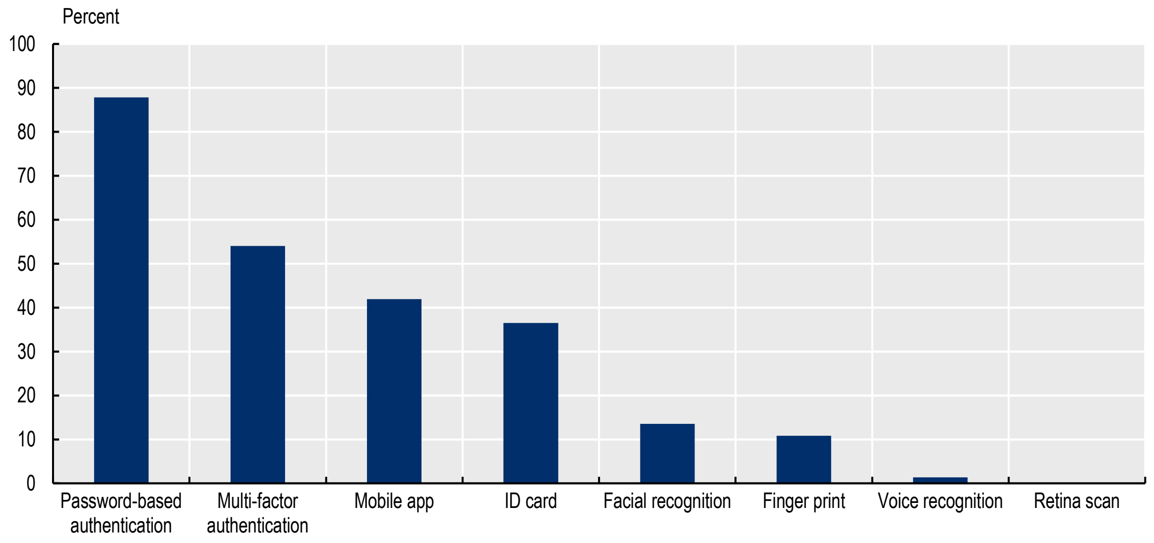
Note: This figure summarises the responses to the question in the global survey on digitalisation: "Of your business taxpayer population, please indicate the estimated percentage that use an approved digital identity to access secure digital services offered by your administration".
Source: OECD et al. (2022), Inventory of Tax Technology Initiatives, https://www.oecd.org/tax/forum-on-tax-administration/tax-technology-tools-and-digital-solutions/, Table DI2 (accessed on 3 August 2022).

Means of authentication

Authentication refers to the process of verifying the attributes of a user and matching them to the digital identity stored within the system. Authentication should be secure and reliable enough to prevent misidentification, but at the same time should display a high level of availability and convenience for users. A vast majority (88%) still supports password-based authentication, while more personalised methods (biometrics) such as finger prints and facial recognition are both being supported by less than 14% of the respondents at present. (Leveraging biometrics for both authentication and ID proofing processes is likely to increase convenience, reliability, and reduce misidentification.)

Figure 1.3. Means of taxpayer authentication methods used by tax administrations

Percent of administrations that use the respective method



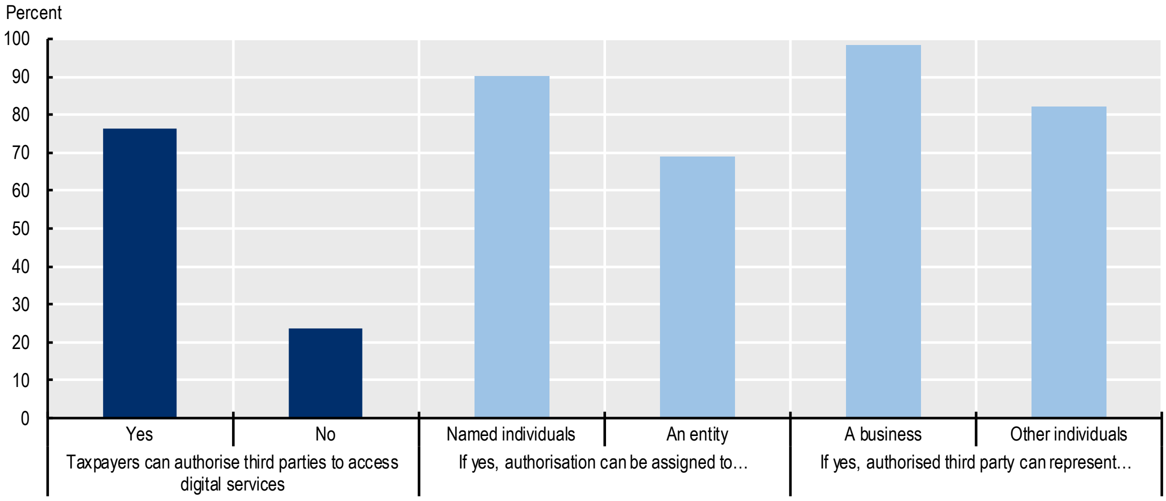
Note: This figure summarises the responses to the question in the global survey on digitalisation: "Please indicate what types of authentication methods are used by your administration"; administrations could choose multiple answer options.
Source: OECD et al. (2022), Inventory of Tax Technology Initiatives, https://www.oecd.org/tax/forum-on-tax-administration/tax-technology-tools-and-digital-solutions/, Table DI5 (accessed on 3 August 2022).

Different tax administration services may require different levels of security, for example making changes to personal information such as address and bank account information may be subject to stricter access controls than viewing information. The data on the Inventory of Tax Technology Initiatives (ITTI) also shows that 60% of tax administration in the database apply different authentication methods based on the level of security required for certain types of interactions, see Table DI5 on ITTI (OECD et al., 2022[3]).

Granting permissions

In addition to direct digital access to tax services, 76% of the tax administrations allow taxpayers to authorise third parties (such as family members or a tax practitioner) to access secure digital services. In 90% of those cases, authorisation can be assigned to a named individual, and in two-third of the cases to an entity. In addition, in nearly all cases, the authorised third party can represent a business, and in 82% an individual. See Figure 1.4.

Figure 1.4. Authorisation of rights to third parties



Note: This figure summarises the responses to the questions in the global survey on digitalisation: "Does your administration allow taxpayers to authorise third parties to access secure digital services?", "Can the authorisation be assigned to a named individual or an entity?" and "Who can the authorised third party represent?"; administrations could choose multiple answer options.
Source: OECD et al. (2022), Inventory of Tax Technology Initiatives, https://www.oecd.org/tax/forum-on-tax-administration/tax-technology-tools-and-digital-solutions/, Table DI6 (accessed on 3 August 2022).

Domestic interoperability

Reports such as the 2021 OECD report *G20 Collection of Digital Identity Practices* (OECD, 2021[4]) have identified that the focus of digital identity has changed from meeting an organisations needs to meeting those of a citizen. An important enabling factor for achieving this was the creation of domestic interoperability and portability. The process of implementing generic, user-centric and portable digital identity solutions has taken place in stages as can be seen in Box 1.1. which contains an extract from the 2021 OECD report which highlights this.

Box 1.1. Extract from the OECD report *G20 Collection of Digital Identity Practices*

The early approach to online identification was every service and organisation independently solving the problem, leading to a multiplicity of user accounts with an associated multiplicity of usernames and passwords and differing levels of authentication. These models helped make the Internet and digital space what it is today but reflected an organisation-centric view of identity that resulted in little or no control for citizens over their identity, and fragmented the ownership and responsibility for their sensitive information and data across multiple organisations.

The first national approaches to digital identity tried to address the issue by creating singular, centralised, forms of identity, rooted in existing analogue proofs. These e-ID efforts saw countries take existing identity infrastructure that included identity cards and population registers and add an additional layer of functionality to physical tokens, through a combination of card-reading hardware and digital certificates. In many countries, this solution was developed in partnership with the private sector, including the financial sector, to allow for the portability and reuse of an identity, and by extension their credentials and data, to access services in both the public and private sectors.

However, the e-ID approach had its own limitations. This was particularly acute for those societies and governments where identity was not based on identity cards or population registers. However, these limitations were also felt in constraining ambitions for transforming the user experience of government and the private sector to be seamless and frictionless. In attempting to address the disadvantages of organisation specific, centralised approaches, a federated model for digital identity was developed as an alternative.

In a federated identity model, a digital identity is not provided by service-specific providers or a single, central solution but through defined trust frameworks and identity standards. These frameworks and standards encourage multiple actors to operate as identity providers (IdPs). Users verify their identity with their choice of IdP and refer to them when they need to access a service requiring identify verification. For those societies without an analogue identity infrastructure of population registers or identity cards, this has become the preferred route to develop digital identity solutions. Federated approaches help to avoid individual organisations developing authentication infrastructure independently, and thus reduces the fragmentation of ownership and responsibility for citizen credentials.

Source: OECD (2021), G20 Collection of Digital Identity Practices: Report for the G20 Digital Economy Tak Force, Trieste, Italy, August 2021, https://doi.org/10.1787/75223806-en

As noted in Box 1.1, many governments are migrating from organisation specific digital identity credentials and solutions towards more open, government and nation-wide systems. Tax administrations are part of that trend and the country cases in Annex A illustrate this.

This trend means that tax administrations need to promote the “development of inclusive, equitable and trusted digital identity solutions that allow citizens to verify and authenticate their identity as easily as possible in any given context” (OECD, 2021[4]).

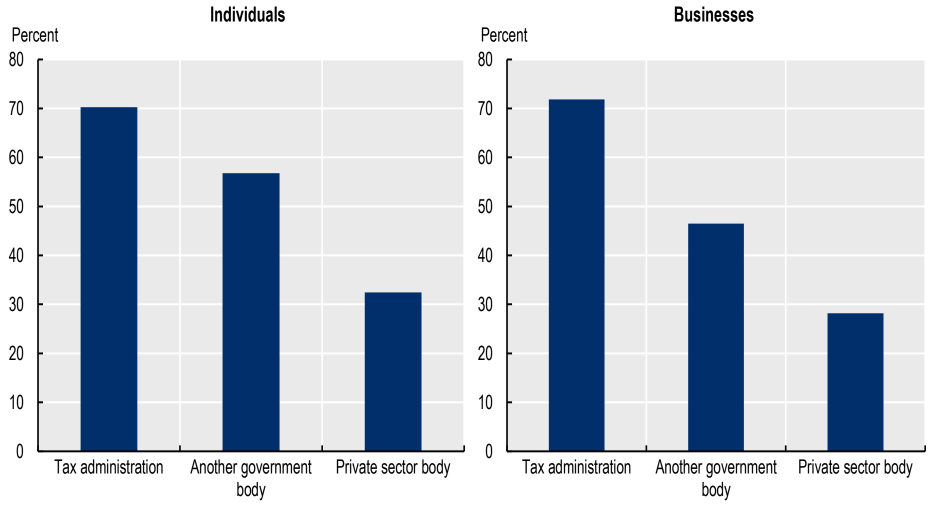
The OECD report *G20 Collection of Digital Identity Practices* concluded that “Digital identity can add the greatest value when it is integrated into the day-to-day life of citizens allowing access to services provided by multiple sectors and countries. It is valuable to continuously reflect on the user experience (including end-users and service providers) in the development and delivery of digital identity solutions. Digital identity can provide citizens with ownership and visibility of how their data is being used and shared in order to encourage them to take greater control over their digital identity and to uphold trust in new and existing digital identity systems. The success of digital identity solutions requires a comprehensive governance grounded on effective legal frameworks, leadership, cross-sector collaboration and resources.” (OECD, 2021[4])

This digital identity path leads to enhanced interoperability between solutions and solution providers supporting secure and unique identification of taxpayers and citizens in an integrated way. This can help to reduce burdens for taxpayers, enabling more “tell me once” possibilities as well as facilitating the movement of processing into taxpayers’ natural systems and the automation of interconnections, including with tax administration systems.

Current picture

Many tax administrations have indicated that taxpayers can use digital identities issued by others than the tax administration itself. Both in case of individual and business taxpayers, approximately half of the administrations indicated that the digital identity provider can be another government body, and around 30% indicated that the digital identity can come from a private sector body, see Figure 1.5. In the case where there are multiple providers, tax administrations confirm high rates of interoperability for individuals (79%) and businesses (73%), see Tables DI1 and DI2 on ITTI (OECD et al., 2022[3]).

Figure 1.5. Digital identity provision



Note: This figure summarises the responses to the question in the global survey on digitalisation: "Who provides the digital identity that individuals and businesses can use to access secure digital services offered by your administration?"; administrations could choose multiple answer options.
Source: OECD et al. (2022), Inventory of Tax Technology Initiatives, https://www.oecd.org/tax/forum-on-tax-administration/tax-technology-tools-and-digital-solutions/, Tables DI1 and DI2 (accessed on 3 August 2022).

Box 1.2. Whole of government, cross-sector examples

Australia

myGovID is the Australian whole of government digital identity solution providing an easy, safe and secure way for an individual to access government online services. An individual downloads the myGovID app to a smart device and establishes their identity to either a Basic, Standard or Strong identity strength. Individuals need to verify their identity against Australian government issued identity documents (e.g. driver's licence, birth certificate) and complete a liveness check and face verification (currently only available against Australian passports), where required. The majority of government online services require a Standard identity strength to access their services. Services with a higher risk of fraud require a Strong identity strength which requires face verification.

myGovID enables a user to log on to any browser based online environment, from a device of their choice, such as a PC, tablet, smart TV etc., providing flexibility in how and where they transact online.

myGovID will eventually form part of a wider Trusted Digital Identity System where multiple digital identity providers will be able to participate. All participants in the Trusted Digital Identity System will need to meet the same standards, which are currently set out under a policy framework (the Trusted Digital Identity Framework) with a view towards creating Trusted Digital Identity legislation. Currently there are 38 government agencies with 125 online services using Digital Identity.

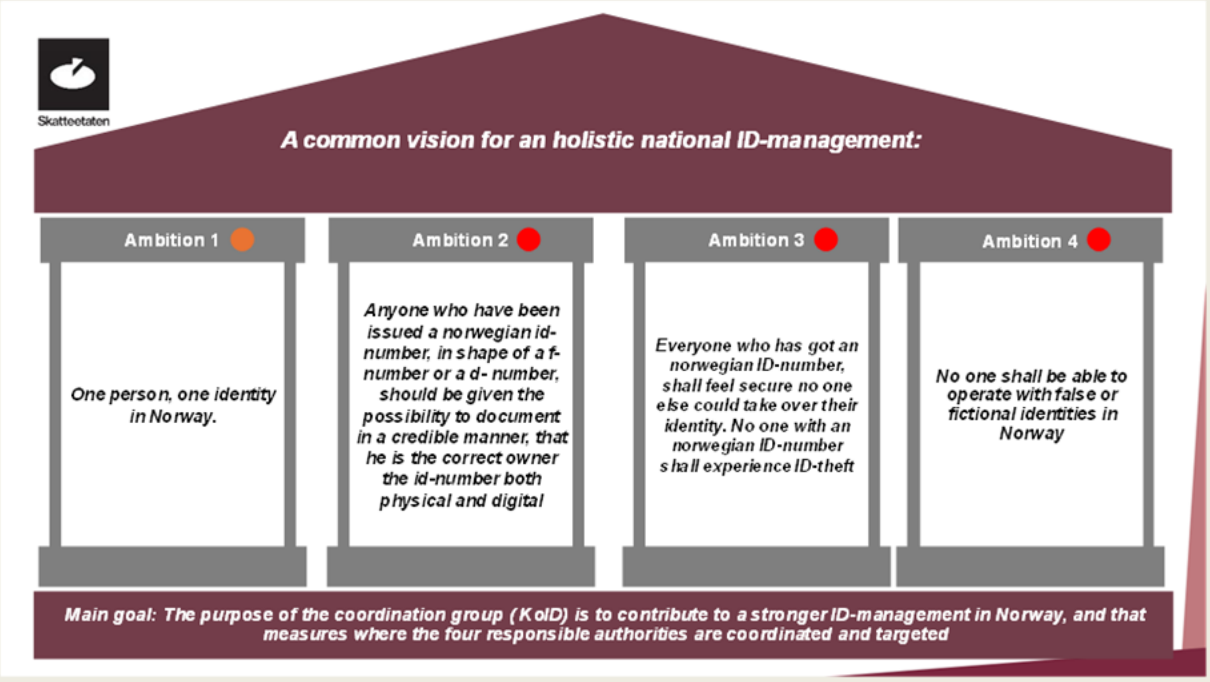
Canada

The ability to transfer from one federal government department portal to another is possible in Canada. The Economic and Social Development Canada department ID proofs a client and permits entry into their (My Service Canada Account – MSCA) portal. From MSCA, a client can link across to CRA's My Account portal without entering additional credentials. Clients in CRA's My Account can similarly link over to the MSCA portal. Both departments co-operate to ensure they are comfortable with each other's identity and credential management processes (established October 2016, making up 10% of CRA's digital users).

Norway

In Norway, the Police Directorate, The Immigration Authorities, The Directorate for Digitalisation, the Norwegian Labour and Welfare Administration, and the Tax Administration have as five of the important stakeholders in the government's identity management, agreed on a common vision for strategic and holistic ID-management. The main goal is to contribute to a strengthened, secure, and more coordinated and efficient id-management in Norway.

Figure 1.6. Towards Whole of Society ID



A common vision for an holistic national ID-management:

Ambition 1: *One person, one identity in Norway.*

Ambition 2: *Anyone who have been issued a norwegian id-number, in shape of a f-number or a d- number, should be given the possibility to document in a credible manner, that he is the correct owner the id-number both physical and digital*

Ambition 3: *Everyone who has got an norwegian ID-number, shall feel secure no one else could take over their identity. No one with an norwegian ID-number shall experience ID-theft*

Ambition 4: *No one shall be able to operate with false or fictional identities in Norway*

Main goal: The purpose of the coordination group (KoID) is to contribute to a stronger ID-management in Norway, and that measures where the four responsible authorities are coordinated and targeted

Source: Australian Taxation Office, Canada Revenue Agency and Norwegian Tax Administration.

References

OECD (2022), *Digital Transformation Maturity Model*, https://www.oecd.org/tax/forum-on-tax-administration/publications-and-products/digital-transformation-maturity-model.htm (accessed on 3 August 2022). [4]

OECD (2021), *G20 Collection of Digital Identity Practices: Report for the G20 Digital Economy Tak Force, Trieste, Italy, August 2021*, OECD Publishing, Paris, https://doi.org/10.1787/75223806-en. [5]

OECD et al. (2022), *Inventory of Tax Technology Initiatives*, https://www.oecd.org/tax/forum-on-tax-administration/tax-technology-tools-and-digital-solutions/ (accessed on 3 August 2022). [3]

2 Cross-border Digital Identification Challenges and Solutions

Cross-border interoperability

Unlike domestic cross-sector interoperability, outside of federated systems (see below) cross-border interoperability is not currently being implemented by many tax administrations globally often driven by differences in systems and levels of maturity in domestic digital identity systems.

This lack of cross-border compatibility of digital identity presents a number of challenges for tax administrations and taxpayers and can make it difficult to realise the benefits envisioned by Tax Administration 3.0 (OECD, 2020[5]) in many cross-border situations. These challenges and impacts may grow as the rapid digitalisation of the economy makes it easier and more common-place to operate across-borders both for businesses and individuals. In order for digital identities to fully support seamless cross-border taxation, it is important to consider the need for:

- *Full scale digital accessibility of all taxpayer services*. Trusted and secure digital identities should enable taxpayers and their representatives to digitally access the full portfolio of tax services. All services should be digitally available without regards to whether it is delivered from the tax administration directly or embedded within services from another government agency or a private sector third party.
- *Unique digital identification of business transaction actors*. Trusted and secure digital identities should support effective mechanisms to uniquely authenticate parties involved in business transactions that are both business to consumer or business to business transactions. These mechanisms should be available to all third parties facilitating business transactions for instance platforms, system service providers and financial institutions.
- *Unique digital identification of asset owners.* Trusted and secure digital identities should support effective mechanisms to identify owners of potentially taxable assets. Mechanisms should also be available to determine ultimate ownerships when assets are owned by companies. Transparency should be maintained in case companies and/or their assets are changing ownership
- *Taxpayer transparency and consent*. In case digital ID's are needed for service delivery, it should be transparent to the taxpayer how and why it is used, and how access to information associated with the identity is limited and secured.

An important factor enabling the longer-term cross-border interoperability and portability of digital identities are the underlying identity infrastructure and frameworks supporting digital identity solutions. The stock-taking OECD report *G20 Collection of Digital Identity Practices* (OECD, 2021[4]) looked, among others things, at the work ongoing across G20 members to realise the opportunities offered by trusted and portable digital identity, with the long term objective of cross-bordery interoperability.

Tax administrations may have different starting points but a number of them has indicated using existing frameworks, such as:

- *eIDAS - EU Regulation (EU) No 910/2014* for individuals (56%) and business (52%);
- *NIST – SP 800-63 (US National Institute of Standards and Technology (NIST) Digital Identity Guidelines*, for individuals (18%) and business (18%).

See Tables DI3 and DI4 on ITTI (OECD et al., 2022[3]).

Box 2.1. Supporting the digial identification in different scenarios

Australia

Documents used to set up a myGovID are 'source verified' against Australian government databases. Individuals who do not have the required Australian documentation can obtain a Basic strength myGovID with a name, date of birth and email address (only the email address is verified). Individuals with a Basic myGovID need to send the ATO certified foreign identity documents in order to obtain limited access to ATO online services. The ATO has undertaken a review of their online services and determined those digital services with a higher fraud risk cannot be accessed by an individual with a Basic myGovID, for example an individual with a Basic myGovID can lodge a business activity statement but cannot update bank account details. Foreign identity documents cannot be used to obtain a Standard or Strong myGovID identity level as they cannot be source verified.

Norway

The National ID-number is given to all Norwegian citizens but also to all residents and non-residents after a set of criteria. There are two main categories of numbers. The F-number is given to Norwegian citizens, residents and children born by Norwegian citizens abroad. D-numbers are given to non-residents with a legal connection to Norway where public authorities or other actors have a need to identify the person.

Spain and Finland

The Spanish platform for identification, authentication and electronic signature, Cl@ve, incorporates identification mechanisms from other countries of the European Union (eIDAS), as they are integrated into the system of cross-border recognition of electronic identities provided for in European legislation.

EU citizens with electronic identification based on the eIDAS regulation can access a limited set of e-services offered by the Finnish Tax administration. In addition, representatives of foreign companies can log into a limited set of e-services by using the Finnish Authenticator app (both EU citizens and non-EU-citizens). Via these limited e-services, one can handle some tax matters, such as sending applications, submitting tax declarations and checking previously sent applications. Tax-related decisions or for example information application process statuses, are not available.

United States

The IRS has an international user population, such as Americans living abroad that continue to have tax obligations to the US government, that is currently supported but the IRS is looking to expand its services to the international user population. The CSPs that the IRS are leveraging are building capabilities within their solution to be able to address account creation, including identity proofing of non-US citizens as well as defining exception processing for any international users that may be unable to successfully complete the account creation process. This additional capability would provide an additional mechanism to ensure that non-US citizens are verified correctly and efficiently prior to being able to access IRS services.

Source: Australian Taxation Office, Norwegian Tax Administration, Spanish Tax Agency, United States Internal Revenue Service.

While the development and usage of such frameworks may offer potential solutions in the longer-term for the cross-border interoperability of national digital identities, at present only around 25% of tax administrations on the ITTI database indicated they are supporting interaction with foreign systems in practice with respect to individual and business taxpayers, many of which are EU Member States under the eIDAS regulation. See Tables DI3 and DI4 on ITTI (OECD et al., 2022[3]).

Stakeholder challenges

The tax administrations which led the work on this report analysed a number of examples of situations where, from their experience, significant issues could arise from the lack of cross-border interoperability of digital identification. These examples are set out in Annex B. To note, though, that these examples should be treated as illustrative since they may not represent the situation in all jurisdictions and, in some cases, practical aspects may be capable of being resolved by policy changes. Further work on the identification of issues arising, including with business representatives, is one of the recommendations of this report. (For that purpose a draft template has been developed in Annex C. The generic issues identified for taxpayers, tax administrations and third parties not operating in federated systems (such as the EU) are set out below.

Taxpayers

The lack of globally interoperable digital identity solutions impacts tax service quality levels, increases administrative burdens and makes it harder for taxpayers to comply with their tax obligations. Challenges can be grouped into three areas:

Limited digital services provided by host country tax administrations to non-residents.

- Fewer services are available digitally, particularly those which involve higher security risks.
- High barriers exist for using existing digital services compared to those for residents.
- Manual and paper processes are often required for non-residents and can be highly cumbersome compared to digitalised process flows, and may lead to extensive delays and costs.

Limited alignment in cross-border taxpayer services between home and host countries.

- The fact that taxable income, business transactions and assets might be taxable in both home and host country is not reflected in tax service support and applications.
- Digital services from tax authorities mainly focus on tax liabilities and taxing rights as regards the domestic tax base.
- The taxpayer will thus generally have limited support to make sure a potential interdependency between tax processes in two countries is handled correctly.

Limited or non-orchestrated cross-border tax services to support global joined-up tax administration processes, such as data exchange.

- Even if some standardised solutions are starting to emerge in some areas, data exchange is still a downstream activity, not automatically connected with the digital identification systems in each country. There is a limited focus on creating joined-up cross border services for the taxpayer.

For citizens engaged in international processes this often implies the management of multiple digital identities, potentially burdensome registration processes and possible delays in claiming and settlement of rights (such as related to deductions and refunds). In many cases, it may be that taxpayers will require the support of professional advisors or agents.

Businesses may also face burdensome, and often paper-based, cross-border identification processes. This can potentially create barriers for entering new markets and doing business abroad, which may particularly impact smaller businesses.

Box 2.2. Taxpayer identification in different scenarios

Australia

The easiest way for taxpayers (who do not utilize the services of a tax agent) to meet their Australian tax obligations is through online services (e.g. lodging an Individual Income Tax Return via myTax). However, these online services require the user to establish a digital identity with a standard strength in the first place and this is not possible for non-residents who do not have any Australian ID documentation. Without this, they are unable to access digital services directly and would need to use a registered tax intermediary to fulfil their tax obligations or alternatively lodge a paper form. The service levels when using a registered tax intermediary or filing a paper form are the same as what a domestic taxpayer would get with these channels. The biggest difference in service levels is the unavailability of direct access to digital services for non-residents.

Finland

In general, strong digital ID is required to access full e-services, i.e. MyTax-online service. Within MyTax, one can handle most of their tax matters. Within Finnish context, “strong digital ID” practically means that one has either online banking ids, a mobile certificate or an electronic ID card (which is not available to non-residents). In other such cases, where a person has not a strong digital ID, options are either limited e-service or to give/receive tax declarations on paper. To access limited e-services, taxpayers have to use Common European identification method or the Finnish Authenticator app. Within limited e-services, one can handle some of the tax matters, such as send applications, submit tax declaration and check previously sent applications. Tax decisions or other information, for example information about processing the application, are not available.

Norway

Non-residents have the same right to digital services as residents, but the process for getting access to digital ID is more complicated. The most widely used digital ID solution in Norway (Bank ID) requires a Norwegian bank account, physical ID-verification and Norwegian cell phone number for mobile verification. Non-residents can use the less used Min ID solution but still have access to most government services delivered by the tax authorities. This requires a set of codes sent on paper to the tax-payers home address in the home country. Even if most services are available in English and support pages on several languages, the barrier to using digital services are considered high, due to understanding how the Id system works and language barriers.

Sources: Australian Taxation Office, Finnish Tax Administration and Norwegian Tax Administration.

Multinational service providers

Many digital platforms, digital market places and financial service businesses operate in a global context, servicing customers residing in many countries. The management and delivery functions of these businesses, which may or may not be third parties, may also be spread over a range of countries as may be the case for marketing, support, data management and logistics. For these businesses, customer identification is a key driver behind their business models. Matching these identities with those included in jurisdiction-specific data reporting formats can be burdensome and may be prone to mistakes.

Tax administrations

The majority of tax administrations' service portfolio and compliance risk management activities focus on their domestic taxpayer base of private individuals, SME's and large businesses, and on income created domestically. When dealing with non-residents, tax administrations are often forced to rely on paper-based communication and assessments, and/or heightened verification processes. Manual ID-checks, the verification of business and tax documents and paper-based or non-integrated audit data can be time consuming and costly activities and can create compliance issues.

Compliance challenges

Maintaining taxpayer compliance is a core function of any tax administration. Compliance risks often emerge because taxpayers make unintended errors in their filing processes. However, a small minority of taxpayers may try and deliberately disguise their ownership of an asset or conceal their identity. Digital identity systems can be helpful in tackling this, by making it harder to not register as a taxpayer or register by using fake or false identities. In addition, it can also help prevent fake or hidden registration of assets abroad, and bring greater transparency to the beneficial ownership of assets.

More challenging can be responding to complex fraud schemes, such as:

- Identity theft of a non-resident individual or entity might be used to obtain a fake identity to commit tax fraud in a host country. With the new identity in the host country an employee can work on someone else's identity and get access to a contractor's workplace without being correctly registered for tax. Weak authentication and authorisation practices can create particular vulnerabilities for these types of fraud.
- The use of multiple identities enables taxpayers to game the system and 'shop' for the lowest tax rates and multiple benefits in a host country. Multiple identities can be either obtained in the home or in a host country.
- Place of consumption fraud occurs in cases where consumers of remote digital services are able to avoid VAT payments by fraudulent authentication or by hiding their real identity.
- Missing trader fraud is a well-known phenomenon in which fraudsters falsely claim an input-VAT credit and/or a VAT-free treatment of their inputs and collect VAT on their outputs which is subsequently not paid to the tax authorities (the trader "goes missing") These types of schemes often use techniques to reduce tax authorities' visibility and understanding of the underlying transactions and to shield the perpetrators against detection, which may include the use of front companies and false or stolen identities.
- Avoiding tax by obscuring beneficial ownership of assets by setting up complex ownership structures of companies and registering these in different countries with representatives of several nationalities. This may be supported by the buying and selling of shares within the structure. Such frauds have been used to evade, inter alia, property tax, capital gains tax, wealth taxes and personal income taxes.

To reduce or alleviate these challenges requires the interoperability of digital identities across borders. As described above, this may become possible in the longer term through the development of compatible national and regional digital identity systems in combination with federated trust frameworks. It may also be possible to develop processes allowing for the digital identity used by a taxpayer in jurisdiction A to be accepted as a trusted digital identity in another one for specified taxation purposes.

This has been explored in the 2022 OECD report *Tax Administration 3.0 and Connecting with Natural Systems: Initial findings* (OECD, 2022[1]). In summary, the work on this report has identified possible options, which require further exploration and development, for creating a common view of the digital identity of taxpayers who use sharing and gig economy platforms in cross-border situations.

Initial work here is looking at the possibility of leveraging existing digital identity systems in each tax administration to create a link between the platform systems and the tax administration systems in respect of authorised information. This would allow one website or application to access the authorised information hosted by another. This would have the benefits of being:

- **Transparent** to the taxpayer, as taxpayers would need to give their explicit permission for their data to be shared between platforms and tax administrations
- **Simple** as it is already in use by tax administrations and platforms alike
- **Open** as it is an open standard available to all
- **Facilitative** as it does not prescribe a particular approach.

Finally, it should be noted that the cross border aspects of digital identity not only involve technical challenges, but also raise legal, and data protection questions too, which would need to be addressed in further work.

References

OECD (2022), *Tax Administration 3.0 and Connecting with Natural Systems: Initial findings*, OECD Publishing, Paris, https://www.oecd.org/tax/forum-on-tax-administration/publications-and-products/. [2]

OECD (2021), *G20 Collection of Digital Identity Practices: Report for the G20 Digital Economy Tak Force, Trieste, Italy, August 2021*, OECD Publishing, Paris, https://doi.org/10.1787/75223806-en. [5]

OECD (2020), *Tax Administration 3.0: The Digital Transformation of Tax Administration*, OECD, Paris, https://www.oecd.org/tax/forum-on-tax-administration/publications-and-products/tax-administration-3-0-the-digital-transformation-of-tax-administration.htm (accessed on 3 August 2022). [1]

OECD et al. (2022), *Inventory of Tax Technology Initiatives*, https://www.oecd.org/tax/forum-on-tax-administration/tax-technology-tools-and-digital-solutions/ (accessed on 3 August 2022). [3]

Annex A. Tax Administration Case Studies

Australia

Domestic context

In 2015 the Australian Government agreed to work across government and with the private sector to develop a Trusted Digital Identity Framework (TDIF) to support the Government's Digital Transformation Agenda. The TDIF policy sets out the standards, rules and accreditation criteria to govern Australia's Trusted Digital Identity System (see below). The legislation is expected to be tabled in Parliament (date pending).

The Australian Taxation Office (ATO) delivered core elements of the Digital Transformation Agenda, myGovID and Relationship Authorisation Manager, in June 2019. Take-up rates have exceeded expectations and of 30 June 2022 (related to a population of nearly 26 million people) there has been:

- 9.8 million downloads of myGovID,
- 8.8 million digital identities were created of which 2.5 million are Strong myGovIDs with 2.5 million successful face verifications,
- 2.2 million authorisations accepted in Relationship Authorisation Manager (RAM), and
- 39 federal, state and territory government agencies with over 124 services now utilising the solution.

The uptake of digital identity went from 1% to 11% between 2019 and 2021 (OECD, 2021[4]) as it was a critical enabler for individuals to remotely access the Australian Governments' economic stimulus measures during the COVID-19 pandemic.

Digital identity management system

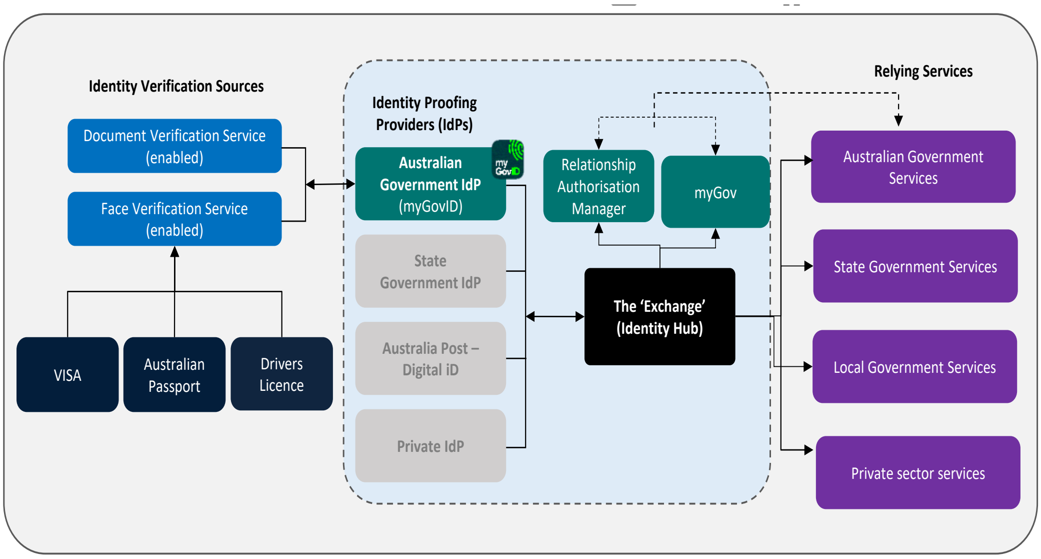
The Australian digital identity solution is a federated identity ecosystem (the Trusted Digital Identity System (TDIS)) providing people with a choice over who they share their identity information with and for what purpose, see figure 6.1.

The digital identity ecosystem consists of:

- Trusted digital identity providers (IDPs). Currently, myGovID is the only approved IDP within the ecosystem. When the Trusted Digital Identity legislation is passed, other accredited providers will be able to join the eco-system, enabling users to choose their preferred provider.
  - IDPs utilise document verification and face verification services to verify a user's identity attributes against trusted *identity documents*.
- The Exchange which acts as a double-blind gate for the exchange of information separates a relying service and the user's identity information.
  - Users select their preferred IDP at the Exchange's "Identity Hub".
  - A service does not know which IDP is being used and an IDP doesn't know which service is being accessed. myGovID and RAM were onboarded to the identity exchange in mid-2021. As a result, 'full' operation of the TDIS is relatively new.

- Attribute providers that work in conjunction with IDPs but are a separate service. Attribute providers represent an authoritative source for a selected set of authorisations, qualifications, self-asserted entitlements, or platform attributes. The ATO has delivered RAM as an attribute provider enabling individuals to be authorised to act on behalf of a business.
- Relying parties that are government agencies or private sector entities participating in the TDIS. They provide online services to an individual using a digital identity.
- The ATO is an identity provider, attribute provider and a relying party. The Exchange is managed by Services Australia on behalf of the Australian Government.

Figure A A.1. Australia's Digital identity ecosystem


Identity Verification Sources
Document Verification Service (enabled)
Face Verification Service (enabled)
VISA
Australian Passport
Drivers Licence
Identity Proofing Providers (IdPs)
Australian Government IdP (myGovID)
State Government IdP
Australia Post – Digital iD
Private IdP
Relationship Authorisation Manager
myGov
The 'Exchange' (Identity Hub)
Relying Services
Australian Government Services
State Government Services
Local Government Services
Private sector services

Source: Australian Taxation Office.

myGovID

The ATO developed myGovID, the Commonwealth Government's identity provider. myGovID is accredited under the Australian Trusted Digital Identity Framework (TDIF). The TDIF strictly controls how identity data is collected, stored, and used by identity providers within Australia's digital identity system and was developed in alignment with the United States National Institute of Standards and Technology SP800-63B.

myGovID is an application downloaded to a smart device that enables a user to prove who they are when accessing government online services. There are two core functions:

- Enrolment: during the setup of a myGovID a user can prove their identity by verifying government issued identity documents (e.g. driver's licence, birth certificate) and using face verification.
- Authentication: after enrolment, a user can logon to online services using their myGovID.

The myGovID mobile app acts like a digital key. Once enrolled, a myGovID enables a user to logon to any browser based online environment, from a device of their choice, such as a PC, tablet, smart TV etc., providing flexibility of how and where they transact online.

To set up a myGovID, the user needs to download the myGovID app to their mobile device (from the Apple app store or the Google Play store) and establish their identity to either a Basic, Standard or Strong identity strength.

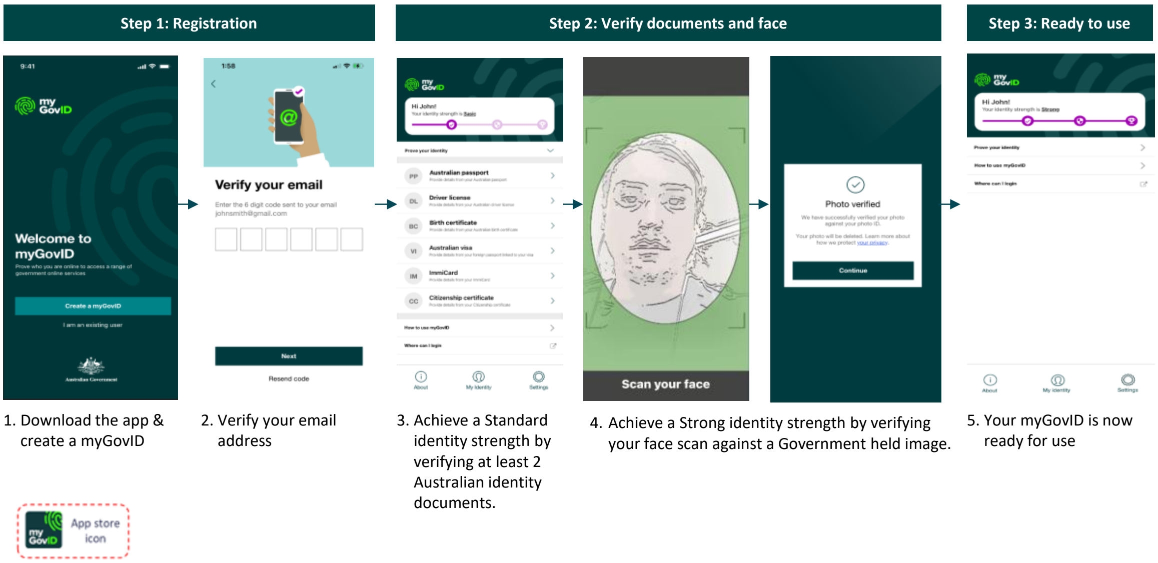
- Basic myGovID (IP1) requires the user to verify their email address.

- Standard myGovID (IP2) requires the user to verify two valid Australian identity documents.
- Strong myGovID (IP3) requires the user to verify two valid identity documents one of which must be an Australian passport (not more than 3 years expired) and successfully complete liveness detection and face verification.
    - Liveness detection enables users to take a ‘selfie’ using their smart device through the myGovID app and ensures the image taken is of a live and physically present person. The image can then, with consent, be used to conduct a one-to-one match against an existing image of that user held by the Government (e.g. passport), to prove their identity.
    - Matching of the newly taken image against a government held image is conducted by the Face Verification Service (FVS) provided by the Australian Government’s Department of Home Affairs. The newly taken image is deleted once the verification process is complete.

When using government online services, a user’s personal information is not shared without their permission – putting them in control of their data. myGovID uses encryption and cryptographic technology as well as the security features in the user’s device, such as fingerprint, face-scan or password. These inbuilt security measures aim to protect the identity of users and help stop other people from accessing their information. Only core identity details are stored in the myGovID app, such as the user’s name, date of birth and email address.

Setting up the Australian myGovID with face verification - individuals have the option to establish the strength of their digital identity during the set-up process (after initial set-up they can upgrade their identity strength at any time). For higher risk services individuals must set up a myGovID with Strong identity strength and complete face verification. In an ever-changing digital world, this world leading capability is critical and is the first in supporting Australians who want secure access to government online services.

Figure A A.2. The use of biometrics



1. Download the app & create a myGovID

2. Verify your email address

3. Achieve a Standard identity strength by verifying at least 2 Australian identity documents.

4. Achieve a Strong identity strength by verifying your face scan against a Government held image.

5. Your myGovID is now ready for use

Source: Australian Taxation Office.

Relationship Authorisation Manager (RAM)

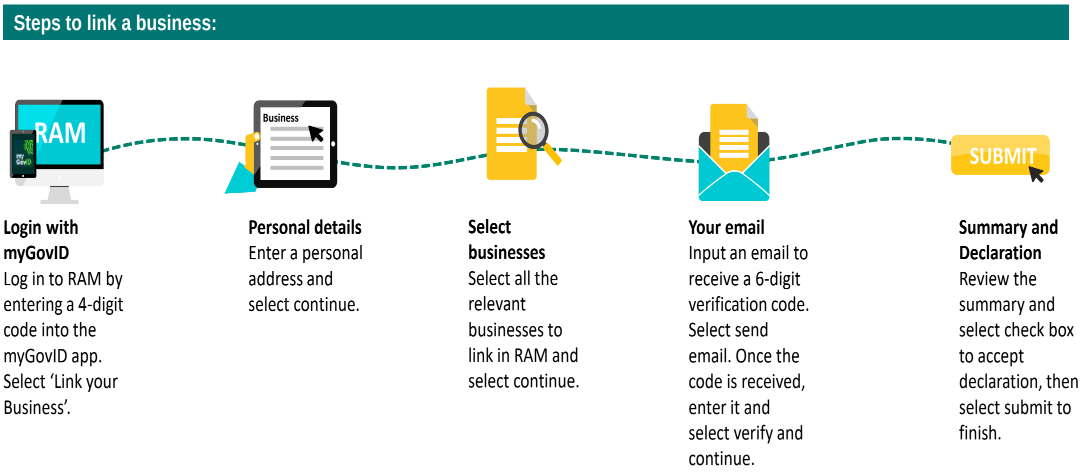
For businesses to use myGovID with participating Government online services, the principal authority of the business (e.g. director or public officer) needs to link their myGovID to their Australian Business

Number (ABN) in RAM. The principal authority is the person responsible for the business as listed in the Australian Business Register.

An individual requires a Strong myGovID to link their business online. Once they have successfully accessed RAM, they are presented with a list of businesses they are eligible to claim. Once the business is linked, they can set up authorisations for others to work on behalf of the business.

Figure A A.3. Using myGovID for business

Setting up authorisations in RAM



Steps to link a business:

Login with myGovID Log in to RAM by entering a 4-digit code into the myGovID app. Select 'Link your Business'.

Personal details Enter a personal address and select continue.

Select businesses Select all the relevant businesses to link in RAM and select continue.

Your email Input an email to receive a 6-digit verification code. Select send email. Once the code is received, enter it and select verify and continue.

Summary and Declaration Review the summary and select check box to accept declaration, then select submit to finish.

Source: Australian Taxation Office.

Challenges and lessons learned

Detailed below are some of the challenges incurred to date and actions taken or in progress:

Societal concerns and debates

Prior to the onset of COVID-19 concerns centred around perceived risk to business from staff potentially accessing government online services on behalf of the business out of hours and off premises. In late June 2020, the ATO developed an Access Report feature that provides tax practitioners and businesses with visibility of when an employee or contractor accesses ATO online services. Lockdowns as a result of COVID-19 eased many of these concerns as businesses saw the benefits of staff being able to access online services from home.

Societal concerns and debates evolved to government oversight and access to citizen data including digital identities. Public discussion and concerns raised on social media has resulted in misconceptions and misunderstandings of digital identity, increasing opposition to legislation that would enable the expansion of the digital identity ecosystem. Legislation is currently being updated based on community feedback and is expected to be tabled in Parliament (date pending).

Enrolment or adoption issues

Only Australian government documents can be used to verify identity to a Standard or Strong myGovID. Businesses initially raised concerns that employees working offshore or Australians without documentation would be unable to achieve the required identity strength to access online services and conduct their work.

- Each agency sets the level of identity strength for their service based on a risk assessment.

- Where an individual is unable to obtain a Standard or Strong identity strength, the ATO provides reduced permissions to access ATO online services to undertake read/review but not edit activities. Access must be first authorised by a business' administrator and subsequently by an ATO officer through the provision of physical identity documents that need to be sighted.

In addition, individuals were concerned with how their privacy would be protected.

- myGovID and RAM are both accredited under the Government's Trusted Digital Identity Framework (TDIF) which ensures they adhere to strict privacy and security controls outlined in law and policy.
- Before myGovID was released to the public, a comprehensive Privacy Impact Assessment was conducted, including a subsequent assessment for Strong myGovID, as well as extensive rounds of security testing which included testing by both ATO security teams and an external provider.

Technological constraints

Technology companies that offered liveness testing solutions were mostly based offshore which raised issues with ensuring data sovereignty. The ATO entered an agreement with the Liveness provider to retain all data onshore.

Legal constraints

Legislation is currently not in place to expand the digital identity ecosystem beyond federal government agencies. Noting, state-based agencies can only access TDIS within a beta-controlled environment and private sector organisations are currently denied access.

Legislation is currently being drafted that will enable the expansion of the TDIS to the private sector and non-federal government agencies.

Canada

Domestic context

Federal departments and provincial/territorial governments in Canada do their own identity proofing, relying largely on shared secrets. However, there are concerted efforts to consolidate activities under what is termed the Pan-Canadian Trust Framework.

The issuance of foundational documents is the responsibility of the thirteen provincial and territorial governments for Canadian born persons. Immigration and Citizenship Canada (IRCC) is responsible for providing documents to those immigrating to Canada. Two provinces currently have digital IDs, with another two on the cusp of implementation. Other jurisdictions are in planning/consultation phases.

The focus of digital ID from the Canada Revenue Agency (CRA) perspective is developing a consolidated approach at the federal level, while consuming provincial and territorial IDs. In the public sphere the focus is on the creation and expansion of the Pan-Canadian Trust Framework (PCTF). The vision is that the providers of foundational identity in Canada (provinces, territories and IRCC) will furnish citizens with digital identities. These identities will be assessed against the PCTF and once 'approved' will be designated as acceptable to parties participating within the framework, including federal government departments. Currently two of 14 jurisdictions have a digital ID approved within the PCTF, and the CRA accepts these digital IDs. The two largest provinces have plans to issue digital IDs within the next 12 months, and the CRA will accept these once approved under the PCTF. The four provinces govern approximately 86% of the Canadian population.

Canada does not have a national ID, but the Canadian government is looking to consolidate digital IDs via the Pan Canadian Trust Framework and Sign-In Canada. Sign-In Canada is intended to become a common credential acceptance platform, which would allow users to access multiple federal departments from the same acceptance platform. A single door providing convenience to users, but also a single door to protect.

Current digital identity management system

The CRA currently offers taxpayers the choice of creating a CRA credential or using a Sign-In Partner, such as a financial institution, to access digital services. ID proofing behind these credentials is carried out by the CRA, and is based on shared secrets. The CRA also accepts two provincial digital IDs. 14.6 million Canadians have an active credential, out of 27 million tax filers. 91% of Canadians file their tax returns electronically.

Service accounts

CRA has three secure online portals: My Account, My Business Account, and Represent a Client.

- *My Account* allows individuals to view their personal income tax and benefit information and manage their individual tax affairs online. My Account for Individuals (MyA) was implemented in February 2005. Individuals were required to create and use a Government of Canada credential called ePass and complete an ID Proofing process in order to map that credential to the individual's account at the CRA.
- *My Business Account* lets business owners (including partners, directors and officers) access their business tax information such as their GST/HST, payroll, corporation income taxes, excise taxes, excise duties and other levies accounts online. In September 2006, the CRA implemented this portal allowing business owners to access business-related tax information. At the same time, functionality was implemented to allow authorised representatives to access, through Represent a Client (RAC), business-related tax information based on the business number.

- *Represent a Client* lets representatives use a secure portal to access tax information on behalf of individuals and businesses. In February 2006, the CRA implemented this portal allowing authorised and legal representatives to access individuals' accounts. This service too, required the ePass and an ID proofing process which identified the would-be representative. Within the 14.6 million Canadians with active credentials, there are 939 438 representatives.

An additional service, Auto-fill my return, is a secure service that allows individuals and authorised representatives using certified software, to automatically fill in parts of an income tax and benefit return with information that the CRA has available at the time of the request. You must be fully registered for My Account to use Auto-fill my return.

Continually adding new services, particularly those that clients indicate they are looking for, has led to a steady increase in enrolment for these portals. Recently, in part because taxpayers could apply for COVID-19 benefits through the portals, usage has significantly increased.

As of 31 December 2021, there have been a total of 154 million sign-ins this year for the three portals: My Account for Individuals, My Business Account and Represent a Client. The chart below provides the yearly sign-ins for each of the portals for 2019, 2020 and 2021.

The pandemic placed a spotlight on digital services and the COVID-19 benefits being offered through the CRA's portals drew increased numbers. For example, sign-ins to My Account increased by 250% from 2019 to 2020 and demonstrated the benefits of digital services. On the other hand, as mentioned, it drew significant attention to our digital services which also became a real target for fraud and identity theft.

Table A A.1. Yearly sign-ins for each of the online portals

My Account for Individuals, My Business Account and Represent a Client

Year	MyA	MyBA	RaC	Total
2019	53 508 764	4 966 279	21 529 267	80 004 310
2020	138 849 224	9 121 194	24 374 726	172 345 144
2021	115 041 012	10 867 197	27 777 517	153 685 726

Source: Canada Revenue Agency.

The initial push towards providing digital services was focussed primarily on a cost savings rationale. Self-service options would reduce the number of phone calls received, and electronic filing would reduce the number of employees (and time) required to process the returns. Over time however, the focus has switched to providing services that clients require or desire, and providing the convenience of self-service that Canadians expect. Also of note, this process has demonstrated that additional digital services do not lead to a reduction in the need for call centre agents. It does, however, allow for increased focus of those call centre agents on value added or complex phone calls, as simple, more transactional requests can be managed online.

For access to My Business Account, an individual is required to go through the same ID proofing as My Account, and then the individual is linked to a business via an existing Business Number. The idea is that there is always an individual on the other end of the keyboard. Similarly, for representatives, identity is based on the individual, and then linked via authorisation to a business or an individual.

An individual or business owner can authorise a representative through My Account or My Business Account. Alternatively, the representative can submit an authorisation request electronically through RAC. The individual or business owner will need to be registered for My Account or My Business Account to use this option. The individual or business owner will need to sign the certification page and send it to their representative, the representative will then submit the signed form in RAC. The business owner or individual will then need to sign in to their account (My Account or My Business Account) to confirm the authorisation.

Credentials

There are currently four means to access CRA's online portals:

1. *Using one of our Sign-in Partners*. Established in 2012. Currently there are approximately 6.5 million users of CRA's portals who sign in using their online financial institution credential.
2. *Using a CRA user ID and password (CRA issued/managed credential).* (Established 2010, approximately 8 million users).
3. *Using a provincial partner (provincial digital ID)*. For this option (making up less than 2% of users), the provincial government establishes the identity of the individual, which is passed to the CRA and bound to a program identifier. (Note the first province, British Columbia, was linked in February 2020, and the second, Alberta, was linked in February 2022.)
4. *Transferring from another federal government department portal*. For this option (established in October 2016), another government department ID proofs a client and permits entry into their (My Service Canada Account – MSCA) portal. From MSCA, a client can link across to CRA's My Account portal without entering additional credentials. Clients in the CRA's My Account can similarly link over to the MSCA portal. Both departments co-operate to ensure they are comfortable with each other's identity and credential management processes. (Link was disabled Aug 2020, but was re-established in 2022. Historically accounted for approximately 10% of users).

For options 1 and 2 (making up 98% of users), the client is ID proofed using shared secrets, e.g. social insurance number (program identifier), date of birth, postal code or Zip code, and a dynamic tax field from a previously filed tax return. In addition, a second factor or out of band code is mailed to the client using the postal service. Digital methods to replace the mailed CRA security code are being examined. The client is then mapped to the digital credential. (Note, these options have existed for 18 years.)

With the Government of Canada (GC) ePass being sunset, the CRA was approached to develop a Credential Management Service (CMS) as a pathfinder project to use as a guide for the next Credential Provider used by the GC. At the time it was thought that CMS might become a replacement for ePass. In October 2010, CRA launched CMS and migrated users who had an ePass to the new CMS credential. CRA has been using the CMS credential since that date. In October 2012, the CRA added a credential broker service 'Government Sign-In by Verified.Me'—previously called 'SecureKey Concierge', allowing Canadians to use the credential issued by their financial institution.

Challenges and lessons learned

There are a number of challenges currently being faced. These include, but are not limited, to:

Balancing off security versus service

Making processes more secure generally results in increased friction, impacting overall service. For example, the second factor in CRA's most common ID proofing process involves mailing a CRA security code to the address on file. This provides additional assurance that the actual taxpayer is the individual registering. However, it does add a delay of 5-10 business days, and is seen by many as an archaic process. The CRA experimented with the option of emailing the security code, but determined this process was vulnerable to fraud/abuse, and so discontinued the practice. The CRA is investigating additional digital solutions to replace the mailed CRA security code.

Moving away from the reliance on shared secrets

The reliance on shared secrets as a basis of establishing identity is becoming vulnerable as more private information is available in the public sphere, presumably moving towards the use of biometrics. Ideally the

CRA would like to get out of the identity/credential management business, but would need an adequate replacement in order to do so. Given there are currently 10 million Canadians with a CRA credential, it will take some effort to move these users to another credential. It is hoped that with the introduction of more and increased use of provincial IDs, the proportion of users of these options will increase.

Enrolling new users

One challenge for using the Sign-in Partners and CRA credential sign-in options is that the shared secret requires the individual to have already filed a tax return with the CRA in order to ID proof. Therefore someone who hasn't previously dealt with us cannot register, a challenge for non-residents or first-time filers.

Integrating third parties

The CRA is working on how to integrate third-parties efficiently into our systems. For example, if a doctor is required to submit a medical certification in order for an individual to qualify for a particular benefit, how do we ensure the identity of the doctor, and ensure they are authorised to submit the information related to a given client.

Privacy concerns

There is a strong culture of privacy in Canada with segments of the population who are very concerned with the information the government has, and who it is shared with. The privacy legislation for the CRA strictly limits the information that it can collect or share, without the explicit consent of the taxpayer. As such, the consent process is particularly important when CRA partners with other digital identity or credential providers.

Finally, in terms of the ultimate Sign-In Canada vision, there has been a challenge to gather the required political will and funding to undertake such a large, whole-of-government approach.

Finland

Domestic context

To identify persons in the registers and information systems of different Finnish authorities, a personal identity code is used. A personal identity code is also used in data communication between different authorities and by private sector actors such as banks, insurance companies, and private healthcare service providers. A personal identity code is issued to a person who is registered in Finland's Population Information System. New-born children in Finland are issued personal identity code without a request, as the hospital provides the necessary details of all births to the Population Information System. For an immigrant moving to Finland a personal identity code is issued when they have been registered in the Population Information System at their own request, or at the time they are granted a residence permit.

Business ID (Business identity code) is used to identify legal persons and entrepreneurs (sole traders). The Business ID is issued by Finnish patent and registration office. A business ID is issued once the businesses start-up notification has been registered at the Business Information system maintained by the Patent and registration office and the tax administration. Business ID can be used to retrieve information about the company; e.g. the registers which it has registered with, the company name (trade name), the company form, address details and tax debt details.

Currently the Digital identity development project aims to develop the electronic identification for Finnish citizens and anyone living in Finland, and to promote the development of functional solutions for identification. Objectives of the project include inter alia to create equal conditions and opportunities for all to use digital identity in social services. Moreover, project seeks to secure the forming and development of conditions for the sharing of personal data, so that digital identity solutions can be based on a core identity guaranteed by the state. The project also facilitates the registration of non-Finnish nationals and their electronic identification in Finland, as well as enable cross-border electronic identification from Finland. Real-time economy project strives to promote the conditions for companies to move to real-time economy. Within real-time economy invoices and receipts will be electronic, for example, and business information will be automatically transferred between different systems. Up-to-date information and its automated processing will increase productivity in both companies and public administration. Digital corporate identity is one of the key building blocks within Real-time economy project.

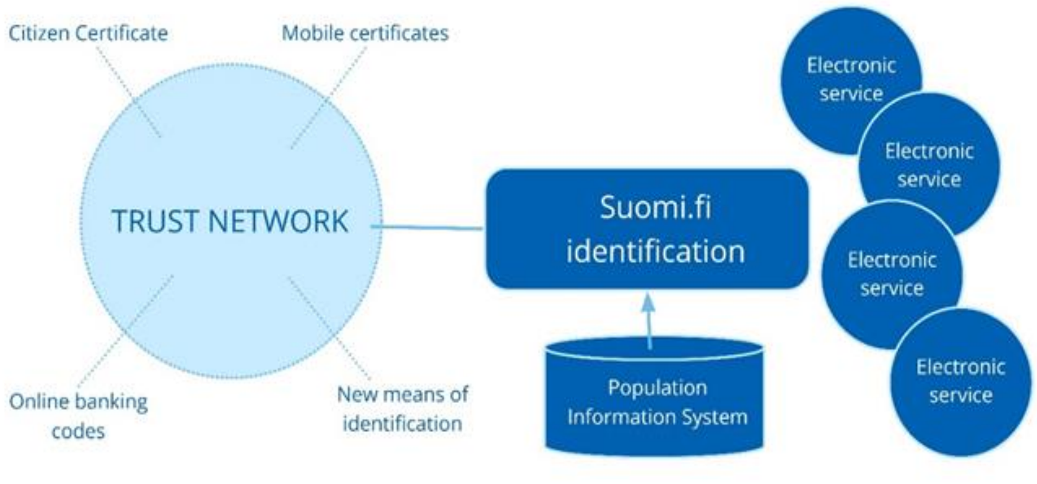
Current digital identity management system

Much has changed after the first versions of pre-completed tax returns, but customer-oriented approach – to bother taxpayers as less as possible - is still relevant. According to its vision 2019-2024 The Finnish Tax Administration aims to be one of the forerunners of digital economy: "We have integrated our services with external business platforms. Taxpayers do not have to concern themselves with taxes, because tax is collected at the same time as the taxable event takes place. Taxation has thus effortlessly merged into our daily lives. The tax gap has diminished and financing for society is on solid ground."

Electronic identification

The current identification system is based on strong electronic identification, which is a means to prove one's identity in electronic services. These identification services must meet certain requirements laid down by law. With strong electronic identification, persons can verify their identity safely in electronic services as the providers of electronic services are able to identify their customers.

Figure A A.4. Trust network and Suomi.fi Identification



Reference: Illustration is based on a publication of Ministry of Finance, Finland.
Valtiovarainministeriön julkaisuja (2019) Sähköinen tunnistaminen: selvitys nykytilasta sekä kehittämistarpeista.

Source: Project Country Case Study Finland.

Suomi.fi identification is mainly used by public electronic services. In practice, online banking codes provided by banks are most established service for electronic identification as it's used by the majority of the citizens. Strong electronic identification services also include mobile certificates issued by telecommunications operators, the Digital and Population Data Services Agency's Citizen Certificate and certain other identification certificates on various organisation cards or registered identification broker services. Identification services are issued for persons. The FTA also provides non-Finnish citizens limited use of electronic services with eIDAS identification means.

Authorisation

To act on behalf of a company, association, or other organisation, one must use Suomi.fi e-Authorisations. In Suomi.fi e-Authorisations, private persons, companies and organisations can authorise someone else to act on their behalf. A mandate is an electronic power of attorney, the details of which are entered in the authorisation register. Authorisation register and Suomi-fi-services are provided by the Digital and Population Data Services Agency. Additionally, in cases where non-Finnish citizen needs to act on behalf of a company, but do not have a Finnish personal identity code or a Finnish identification token, a separate Finnish Authenticator Identification Service can be used.

Identity supported tax services

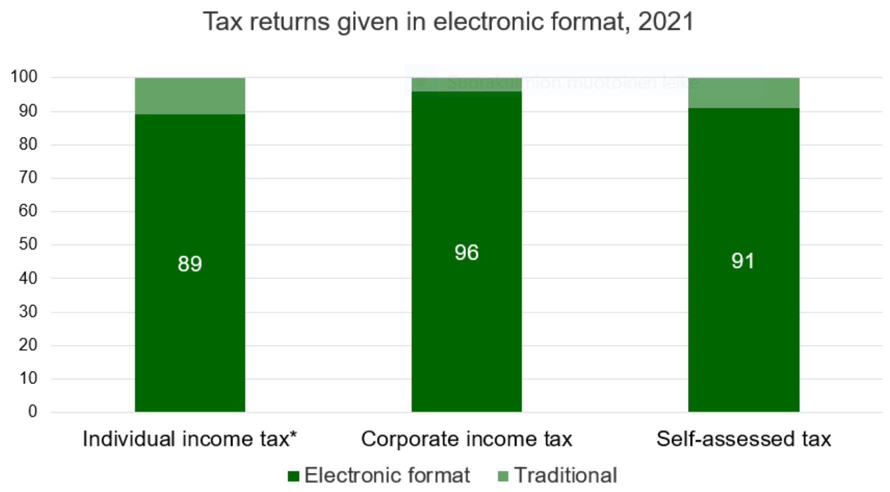
Identity supported tax services include:

- MyTax – an online service where tax returns can be filed including digital customer service. MyTax covers the majority of tax matters. Necessitates a strong electronic identification.
- Ilmoitin.fi - a web gateway for electronic submission of software-generated tax filings that are set up according to the specified formats.
- API's – software interfaces that enables data transfer from customers' software to the Finnish Tax Administration and vice versa.
- Palkka.fi – A free payroll service.
- Lomake.fi (currently in use)

- Electronic filing of returns and requests (Limited use of electronic services with eIDAS identification means).

The e-service is used to request refunds of the tax withheld at source on dividends, interest or royalties (for individual and corporate taxpayers), to submit an application for a tax-at-source card if your corporate entity receives dividends, interest or royalties from Finland (for corporate taxpayers only), submit several annual information returns, submit requests for specific documents, ask for a pre-emptive discussion to be arranged (available to corporate taxpayers), send a deed of inventory of an estate of a deceased person, and submit other requests connected to the inventory deed.

Figure A A.5. Digital identity supported tax services



*) Bar chart on individual income tax includes only customers who made changes to pre-completed tax return. All individual tax-payers receive a pre-completed tax income return. 76% of all individual income tax returns did not require any action from the customer.

Note: “Number of tax returns 3.3 million; of which electronically received 3.2 million. 96% received in electronic format and 4% in paper form”.
Source: Finnish Tax Administration.

Existing electronic services enabled to handle taxation and arrange customer service successfully during COVID-19 crisis. During 2020, taxpayers were more actively using online services (like i.e. MyTax) than during previous years. There was a record to the MyTax service of 25.3 million log-ins that year. At the same time, phone calls and visits to tax offices declined further.

Challenges and lessons learned

There are a number of challenges currently being faced. These include, but not limited to:

Digital identification of businesses

Companies do not yet have a digital equivalent in a digital world and therefore it's more difficult to link data to them or develop functionalities that do not require a person as a user. There is a need for digital identity also for legal persons. Further, data related to a certain individual or a company lies in the databases of different authorities and organisations: digital identities are tied into a certain context - such as taxation. In practice, these contextual identities are not compatible or interoperable thus there is a need to combine these contextual identities in a reliable manner.

Common understanding

There is a need for common terminology to build a basis for common understanding to enable compatibility and standardisation. Cross-administrative cooperation for digital identity is still evolving, yet the understanding of the need for digital identity for both individuals and legal persons is growing.

Change management

Reasons and benefits of a change need to be communicated in a customer-oriented manner: customers are more likely to adopt new tools and support new practices if they offer real benefits, like paperless, user-friendly process. With respect to service providers, in the development phase the main concern for a business might be uncertainty on how this change affects the business: whether there are potential benefits, added value to customer, new business opportunities, risk to the existing business, costs and perhaps most important how user-friendly the solution will be.

Indonesia

Domestic context

As mandated by Law Number 23 of 2006, the Indonesian Government has decided to implement a Single Identity Number. The project was started with the introduction of the Electronic National Identity Card.

In 2007, the Indonesia Government introduced a 16 digits National Identity Number or NIK. It was designed to replace and unify a variety of IDs issued by the local government. Biometric identity (i.e., iris recognition and fingerprint) is attached and able to be used nationally. The measure would solve the issues of double IDs and ensure that all Indonesian were legally registered since they were born.

Government agencies and private sectors gradually take NIK compulsory as part of their verification business process. Over the years, although not literally stated, NIK has been a digital ID for many business processes. With regards to its reliability and uniqueness, NIK has been required by Directorate General of Taxes (DGT) for the tax registration process. NIK is the key of many databases available, providing detailed information on Indonesian activities.

With an effect of Law Number 7 of 2021 on Harmonisation of Tax Regulation, DGT decided to reform its strategy on Taxpayer digital identity by using the national identity. Prior to its implementation in 2022, some adjustments were made to DGT business processes. The changes are expected to serve as a potential leap to a better tax administration system.

Current digital identity management system

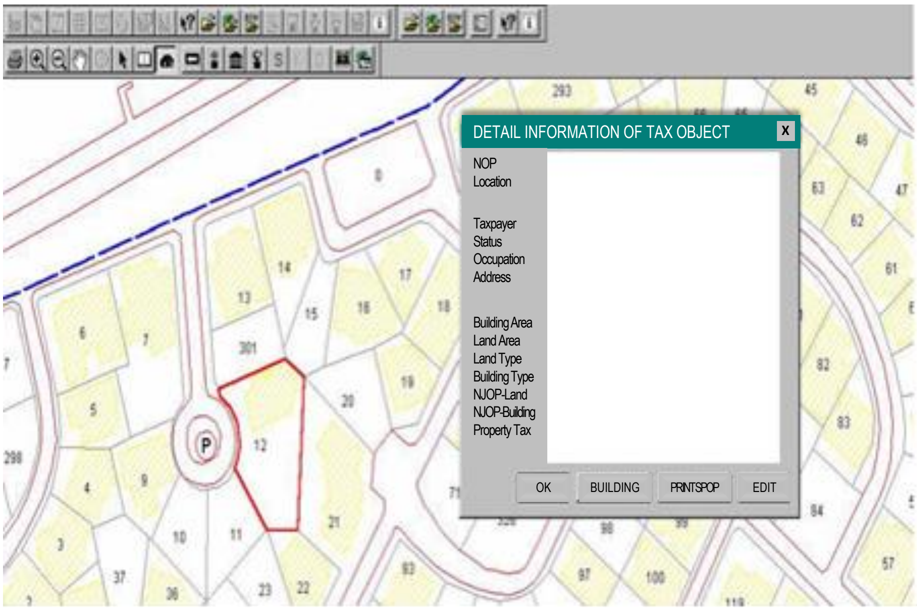
Indonesia’s Directorate General of Taxes (DGT) identifies Digital Identity as one of the core instruments to increase its tax ratio. Finding the best scheme for digital identification has been an ongoing project since 2001. During that process, there are many aspects, opportunity and challenges considered to optimise the tax administration business process.

Property Tax Identity as Group Tax Unit (2001-2006)

Similar to other single identity number projects, Indonesia’s Single Identity Number strategies aim at linking all IDs of each person/entity. Before having the national identity to interconnect entities, DGT used the Land and Property Tax ID (known as “NOP”) as a Group Unit Tax. As a group tax unit, NOP connects entities’ different IDs. The decision was relatively uncommon, but there were advantages, such as:

- NOP represented a single-specific property.
- DGT had a map to locate every NOP as the database to verify the land or property (see figure 6.4)
- Most properties were residential, and each person had different ID’s (i.e., personal ID issued by local government and a driver’s license).
- Some properties were connected with different IDs, such as land certificates, building-permit, the electric bill, and tax ID.
- A person/entity could have more than one property, allowing data integration between entities that share the properties.

Figure A A.6. Map of property tax on 2005



Source: Indonesia's Directorate General of Taxes.

The project was running well for five years, but improvements were necessary since:

- Conventional data collection (i.e., door-to-door survey) and data entry required a significant amount of human resources and administration cost.
- During the data entry process, human resources and software must follow and declare the basic rules.
- Training of data entry targeted much personnel.
- External staff were hired as data collectors to anticipate project delay and domestic resistance

The Permanent Tax Identification Number

Indonesian Taxpayer Identification Number (NPWP) is the number provided for a registered Taxpayer and used as the identification form of the Taxpayer's compliance (Article 1 point 6 of Law Number 28 of 2007). Every individual, company, or entity satisfying the subjective and objective requirements should register for an NPWP. However, several conditions make an entity to have more than one NPWP, or, conversely, more than one entity to have one NPWP.

For individual taxpayers, only one NPWP is required for every Family Tax Unit. However, every family member can register and have NPWP if they decide to separate assets or live separately. The rule also applies when a person registers their businesses in different tax office regions. As for corporate Taxpayers, companies that choose not to centralise their tax reporting should have NPWP for every branch.

NPWP comprises unique digits, tax office code where the taxpayer is registered, and branch code. Such digit classification gives less flexibility for Taxpayers to move their business location, as they must report the changes to the tax office to get new NPWP digits. Also, DGT would bear an extra administrative burden when new tax offices were established since office digits in Taxpayers' NPWP must be converted to the new ones.

In 2015, therefore, DGT implemented permanent digits of NPWP to simplify and improve the tax registration system based on the Director-General of Taxes Circular Letter Number-44/PJ/2015. NPWP digits do not change, although a Taxpayer moves to a different tax office location. Such administration simplicity also improves data integrity and optimises tax services, supervision, and law enforcement.

DGT also has supplemented NPWP with some supporting tools such as the use of:

- Electronic Filing Identification Number (EFIN) as a means of identification since 2002. EFIN is an identity number issued by DGT to Taxpayers conducting Electronic Transactions with the Directorate. Taxpayers can conduct Electronic Transactions with DGT through the Online Tax Service to carry out their tax rights and obligations. To be able to register with the DGT Online or the Electronic System provided by the Electronic Tax Return Service Provider, the Taxpayers need to apply for EFIN activation.
- Digital signature for creating a tax invoice since 2014.
- Digital signature for reporting an annual income tax return since 2021.

The decision to integrate the National Identity and Tax Identification Number is based on the following factors:

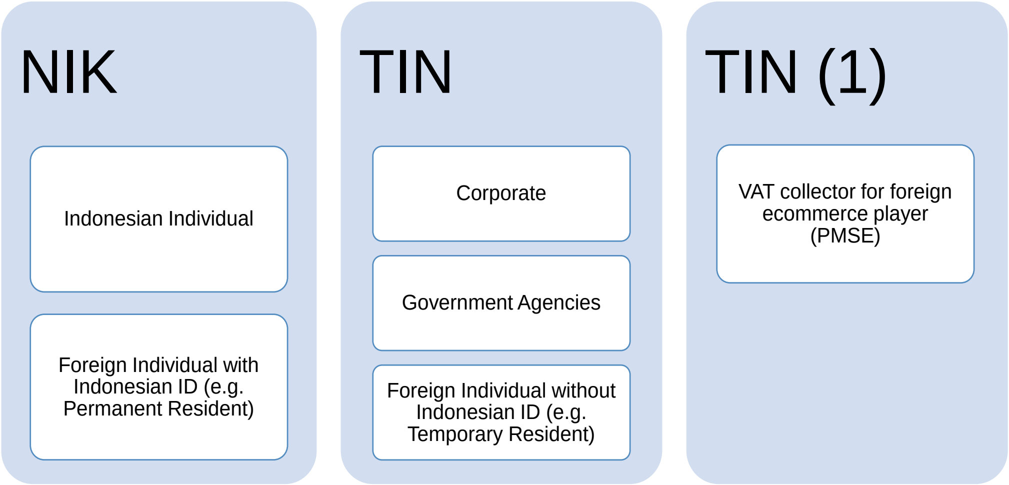
- to improve the identification and registration process of Taxpayers and deal with the shadow economy effectively (OECD, 2017[6]);
- to provide broader government support (i.e., incentive, cash transfer, and job support during the COVID-19 pandemic);
- to carry out seamless tax administration and tax-compliance assessment for taxpayers;
- to support national database policy for better planning, implementation, evaluation, and control of government strategies.

Current implementation

Since 2007, Indonesia NIK has supported seamless taxation business processes. It is designed as the primary key to most information in Indonesia. An individual tax resident will no longer have Tax Identity Number (TIN) by early 2022. The new digital registry will refer to the available NIK data, which consists of information of family and citizenship identity.

Strategically, the new policy to partially replace Tax Identity Number (TIN) with NIK would address the problem of double administration between the Civil Registration Agency and the Tax Administration. Also, the integrated identity approach would help to track the unregistered Taxpayers. However, an exception is made to corporate Taxpayers and Permanent Establishments. They are still required to have the Tax Identity Number (TIN).

Figure A A.7. Use of the National Identification Number (NIK) and the Tax Identification Number


NIK
Indonesian Individual
Foreign Individual with Indonesian ID (e.g. Permanent Resident)
TIN
Corporate
Government Agencies
Foreign Individual without Indonesian ID (e.g. Temporary Resident)
TIN (1)
VAT collector for foreign ecommerce player (PMSE)

Source: Directorate General of Taxes Indonesia.

Different registration procedure also apply to entities appointed as E-commerce VAT Collector according to the Regulation of the Minister of Finance Number 48/PMK.03/2020. Considering their lack of physical presence in Indonesia, deeming such entities as Indonesia tax residents would conflict with the Double Tax Agreement. Therefore, a special registration identity is designed for allowing foreign merchants or service providers to collect VAT on e-commerce transactions. The use of Digital ID for foreign entities appointed as E-commerce VAT Collector also aims at levelling the playing field between digital and conventional business. The system maximises the role of digital platforms in collecting VAT on digital transactions based on a sole-liability regime.

Integrating NIK and TIN will improve the tax administration and public service system. The objective is associated with the Tax Administration Reform program in Indonesia. Not only is it the main priority of the Tax Reform program, but the integration is also expected to bring technological advancement. It provides new tools and methods for establishing better data management of integrated identity number for the sake of a more effective and efficient administration system.

Also, the project receives wider government support and is a part of the national program of “Satu Data” (or One Data). Since data integration among government services’ databases is likely possible, interoperability with external parties could be done more efficiently.

Challenges and lessons learned

There are some challenges encountered during the planning phase of the NIK and TIN integration project.

- Firstly, updating NIK data in the available Taxpayer Master File database requires a significant time and effort. Mainly due to inconsistencies in NIK and TIN data matching.
- Secondly, adjustment of data elements calls for intensive coordination and cooperation with external parties. Not only will the changes impact the DGT business processes, but they will also affect other agencies/parties’ databases, for instance other agencies under the Ministry of Finance (like i.e. Customs and Directorate General of State Assets Management) and institutions appointed to receive tax payments (Banks, Post Office, and others)
- Thirdly, the transformation of conventional TIN to digital NIK raises issues on IT details and the business process level. One of which is the multi relationship joint of TIN and NIK. The previous

model of TIN allows an individual to register with different TINs. This causes several data migration issues.

- Lastly, the integration project triggers security and confidentiality concerns. The process should be done cautiously to avoid data corruption and data breaches. Data protection through encryption helps to ensure good data security in the integration.

Norway

Domestic context

Digital identity for the use of governmental purposes, as well as communication with the Tax Administration consists of an identification and an authentication part.

In order to get a digital identity in Norway you need a national ID-number issued by the National Population Registry. This number is used to identify the person operating in their own capacity, but also when they represent another person, a company, or an organisation. The use of a national ID-number as a basis for a digital ID is required by law both for access to government services and private sector services like banks and telecommunication.

“ID-porten” is a centralised gateway to digital public services. Through one hub, people can access digital public services using their preferred eID-solutions. There is one harmonised login screen for all public services. The gateway itself is developed by the Directorate for digitalisation, but there are various trust service providers delivering eID-solutions from which the person can choose from.

“ID-porten” is a micro service which only performs authentication - eID vendors perform the actual authentication. eID vendors have been selected after a thorough procurement process with complex technical and legal requirements. “ID-porten” simply forwards the authentication from the chosen eID vendor.

The way it is built makes it easy to add and remove eIDs when vendors in the market change. “ID-porten” hides the complexity of eID vendor specific integration. BankID is one of them, provided by the Norwegian bank sector. “MinID” – “MyID” – is a governmental-product.

The volume of logins to “ID-porten” from citizens has increased substantially through the years. In 2020, the volume was 240 million logins with a population of 5.5 million persons.

All digital services from the Tax Administration are connected to this digital identity solution.

Identity management in Norway is spread across several government agencies. As owners of the National Population Registry, the Norwegian Tax Administration is involved in shaping whole of government/whole of society strategies for digital identity. Several processes will eventually shape the Norwegian digital identity solutions for the future.

Current digital identity management system

Identification

The National ID-number is given to all Norwegian citizens, residents and non-residents after a set of criteria. There are two main categories of numbers. The F-number is given to Norwegian citizens, residents and children born to Norwegian citizens abroad. D-numbers are given to non-residents with a temporary connection to Norway where public authorities have a need to identify the person.

At the core of the Norwegian Tax Administration perspective is the aim to create digital identities that are uniquely connected to the physical person. This introduces discussions on different ways of using biometrics to ensure this connection.

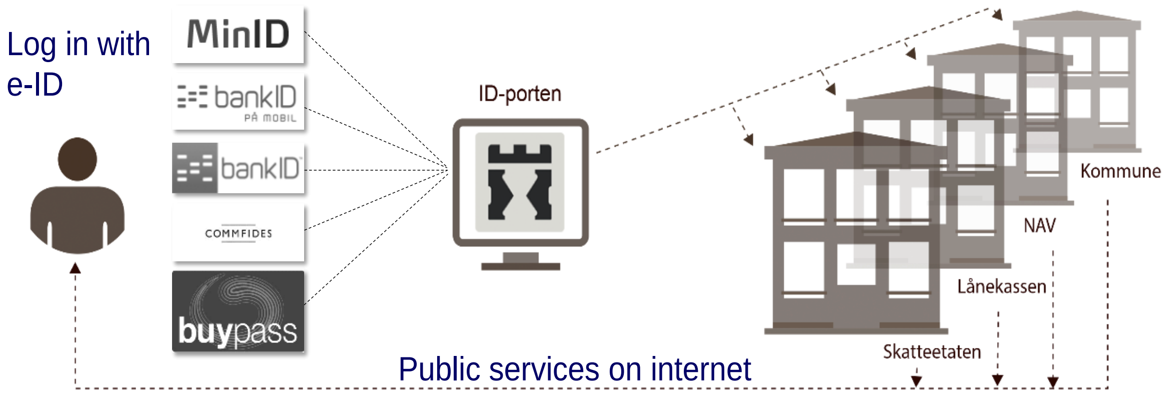
Authentication

“Min ID”

“Min ID” was introduced as a whole of government digital ID solution in December 2008, and “ID-porten” as authentication portal in its first version was developed. The Norwegian Tax Administration started using the solution on a large scale in 2009.

Figure A A.8. The Gateway to public digital services

Success factor - a micro service which only performs authentication



Source: Norwegian Tax Administration.

To start the enrolment process individuals must order a pin code letter from the Digitalisation Directorate. The letter is only sent to the individual's home address registered in the National Population Registry. The pin codes can be used to create a profile with password, e-mail address and phone number. With future logins access codes being sent to the registered cell phone.

To speed up the "Min ID" enrolment process, instead of getting security codes in a letter to their home address, it is possible for ID-checked individuals to get access code for establishing "Min ID" directly on their cell phones while physically present at a Tax Administration office. This solution is called "Min ID on the fly".

"Bank ID"

Digital ID-solutions for the private sector are based on ID-numbers from the government - as required by law - but designed differently and issued by different public and private sector actors for different use.

At approximately the same time as "Min ID" was developed for the public sector, the private sector digital ID solution branded "Bank ID" was developed for access to banks. In 2012 "Bank ID" was made compatible with "ID-porten" along with other digital ID-solutions like Commfides and Buypass. This compatibility - one unified solution for private sector and public sector authentication - stimulated an increase in volume of digital services. "Bank ID" is issued by a company owned by a group of Norwegian banks. In 2021 "Bank ID" is the de facto standard for people getting secure access to digital services in Norway, private or public.

BankID Norway is an independent company – the key success factor is that the eID is broadly recognised by all banks and in the public sector. BankID Norway provides all the banks in Norway with one commonly recognised eID solution. Customer authorisation is not a competitive factor between the banks, but a common eID scheme has big economies of scale which benefits all the banks. One common national solution - only one password to remember - makes it easier and more customer friendly. 95% say "BankID" is easy to use.

"Bank ID" is an integral part of the application for a bank account with an associated debit and credit card, for a bank operating in Norway. When you have a bank account you can apply for a "Bank ID".

Authorisation

“Maskinporten” is a government owned gateway where all access to government information embedded in external services are confirmed. “Maskinporten” is used as a public sector authentication and authorisation mechanism when digital systems from different branches of government communicate with each other through Application Programming Interfaces. It is also used when information from the government is authorised to be embedded in private sector services. “Maskinporten” also limits access to the information a specific service requires.

Operating on behalf of a company

As part of company registration in Norway there is an associated registry with information about people assigned different formal roles in the company. Typical examples are CEO, Managing Director, Auditor etc. When people are assigned to the formal roles, they get access to a set of predefined roles in the government’s solution that matches their formal role in the business. There are also predefined roles that are more limited or specialised to match size, organisational structure, and real responsibilities in the company. Roles can be granted and revoked in a relatively flexible manner. Roles are assigned to an individual by connecting a corresponding internal predefined role to their personal identity F-number/ D-number in the Norwegian Population Registry.

When operating on behalf of the company in the digital space with the government, the person then has to login to government services using their personal electronic ID, for instance “Bank ID” or “Min ID”. At the time of login you can select whether you operate on behalf of yourself as a private citizen, or on behalf of someone else - for instance the company that has granted you a role.

Challenges and lessons learned

There are a number of challenges currently being faced. These include:

- Governance. Lack of a holistic identity management makes it difficult to reach strategic decisions that involve several government agencies.
- Identity theft. As part of the process of getting a digital ID at the highest level of security, you must show a valid Norwegian or international ID- card at the pickup point to get registered. To get a “Bank ID”, the mail pickup point uses special equipment to check the validity of the ID-card. We have seen that it can be a challenge to discover imposters, where someone is using someone else’s ID-documents.
- Digital inclusion. Without ID-documents it is not possible to get access to a digital identity at the highest level of trust. Some services require the use of a digital identity at the highest security level, and certain groups are because of this excluded from accessing public services online.
- The bar for security for public service is often set at the level where people with rights and obligations are able to access services digitally. The alternative is physical and less efficient solutions for those who are not able to fulfil the security demands.
- Costs. Given new developments in markets and technology, there is a debate about whether the current business model will stimulate innovation of new ID-solutions and new digital services.

Spain

Domestic context

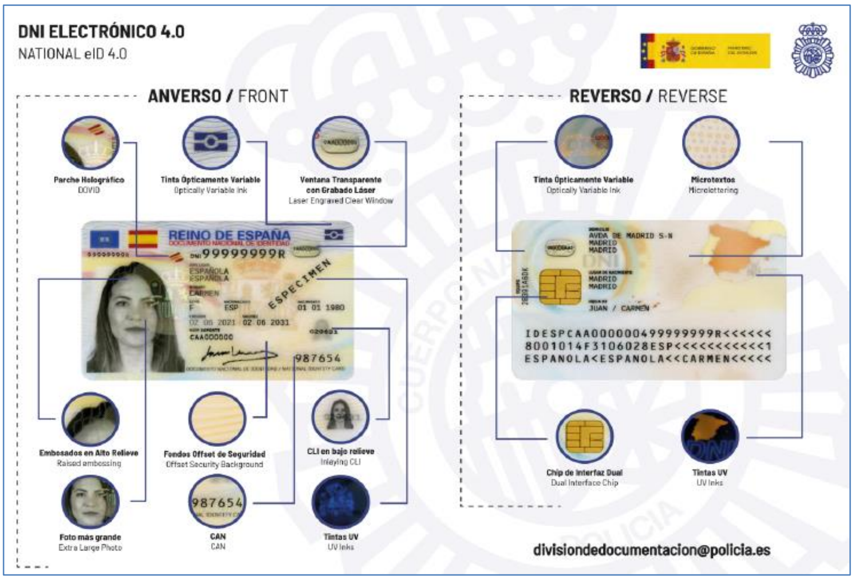
Spain has a National Identity Document, DNI, which is mandatory for everyone over 14 years of age. It is a physical identity card, which is also digital, since it has a chip inserted with an electronic certificate, for all citizens. Therefore, in Spain all individual persons over 14 years of age have a digital identity.

In Spain, in the case of natural persons, the tax identification number NIF (NIF = TIN) coincides with the national identification number DNI (DNI = NIF = TIN), which is mandatory for all persons of legal age, voluntary for minors, although each time it is obtained at a younger age.

The role of the population registry has been fundamental. It has always been based on the census of the Police (Ministry of the Interior), which is responsible in Spain for registering the population. In turn, the Police are responsible for the National Identity Document (DNI) and, therefore, the electronic DNI.

Figure A A.9. National Digital Identity

The new Spanish DNIe 4.0 – European Format



Note: Since June 2, 2021, Spain complies with the criteria established in the European Regulation.
Source: Spanish Tax Agency.

In Spain, 67% internet users actively participate in e-government services, compared to 64% of the EU average.

Current digital identity management system

Both the Tax Administration and the Social Security Administration have several digital identity systems developed over several years. Interoperability with the different digital identity systems is carried out through the public service called "Cl@ve" ("Key" in Spanish). The Cl@ve National Registry is implemented by the Tax Agency and Social Security systems, being a service of the General Secretariat of Digital Administration, which is the national body for the digital transformation of the Public Administration (Whole of Government). The Cl@ve system was approved by Agreement of the Council of Ministers, at its meeting of 19 September 2014.

The Spanish Tax Agency (AEAT) is linked to the national digital identity service (and is part of its infrastructures and services), “Cl@ve”.Therefore, the evolution of the AEAT's digital identity will come from the evolution of “Cl@ve”.

In the specific case of the Personal Income Tax, given its large volume, the AEAT continues to offer authentication based on shared keys. It consists of requesting the taxpayers a specific data from their return from the previous year, which together with the DNI data allow to give them a key, called "reference number", so that they can obtain their tax data, their pre-filled return and also to file their return (see Table A.2).

Table A A.2. Use of means of authentication per tax type

Tax	Authentication	%
Income Tax	Electronic certificate	10.3%
Income Tax	Cl@ve PIN	10.4%
Income Tax	Reference number (shared key)	63.3%
Income Tax (thru representative)	Electronic certificate	16.0%
Corporate Tax	Electronic certificate	100.0%
VAT	Electronic certificate	97.6%
VAT	Cl@ve PIN	2.4%

Source: Spanish Tax Agency, 2021.

The purpose of this "reference number" authentication is to facilitate the compliance of the largest number of taxpayers with their personal income tax obligations, until they migrate to the national digital identity system "Cl@ve".

The Cl@ve system

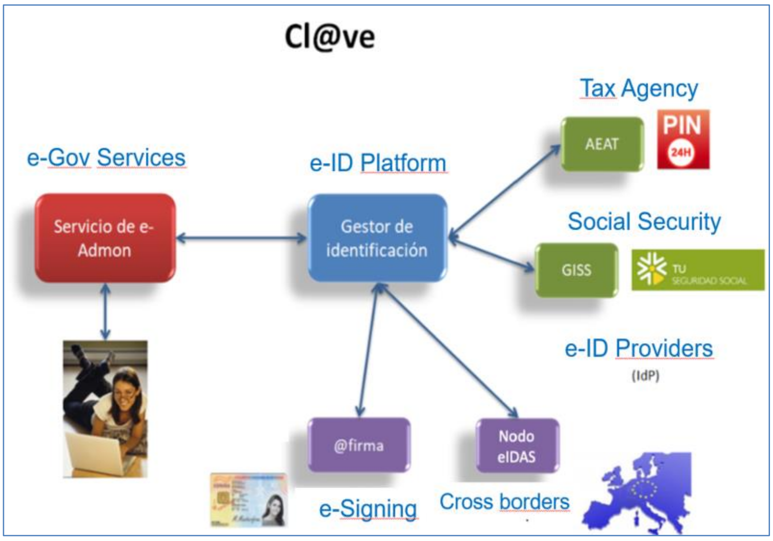
Cl@ve is a system aimed at unifying and simplifying citizens' electronic access to public services. Its main objective is that citizens can identify themselves to the Administration through concerted keys (user plus password), without having to remember different keys to access the different services. Cl@ve complements the current access systems through DNI-e and electronic certificate, and offers the possibility of signing in the cloud with personal certificates guarded on remote servers.

It is a common platform for identification, authentication and electronic signature, an interoperable and horizontal system. Cl@ve avoids public administrations having to implement and manage their own identification and signature systems, and citizens having to use different identification methods to interact electronically with the Administration. Cl@ve allows e-government applications to define the level of assurance in the quality of the authentication they want, based on the data they process and the security classification following the recommendations of the National Security Scheme ENS (Royal Decree 3/2010).

With regard to identification and authentication, Cl@ve adopts the approach of a system of federation of electronic identities, integrating different actors (see also Figure A A.10.):

- E-Government Service Providers: Entities that provide e-government services and use the platform for the identification and authentication of citizens.
- Identification and Authentication Service Providers (IdSP): Entities that provide identification and authentication mechanisms for citizens to be used as common means by other entities.
- Gateway / Identification Manager: Intermediary system that enables service providers to access the different identification mechanisms.

Figure A A.10. The Cl@ve architecture



Source: Spanish Tax Agency.

According to this design, service providers only have to integrate with the Identification Manager, which is in charge of establishing the relevant relationships with the different identification systems. To this end, trust relationships are established between the different actors that integrate with each other, supported by the exchange of electronic certificates and the sending of signed messages between them, which guarantee the secure transmission of information throughout the identification and authentication process:

- The citizen user of the e-government services can choose the identifier they wish to use from those available for the level of assurance required by the application.
- Technically, public eGovernment service providers, through SAML v2.0 message exchange (eIDAS format), describe its architecture as a federated authentication platform.
- Applications do not need to store user data, so the platform provides a "single sign on" SSO system.
- The standards used are SAML 2.0, using XML tickets encrypted by public key.

Registration in Cl@ve

Cl@ve is an electronic identity verification platform for the identification and authentication of citizens. It allows citizens to identify themselves before the Public Administrations with full security guarantees. For this citizens have to register, which can be done in three ways:

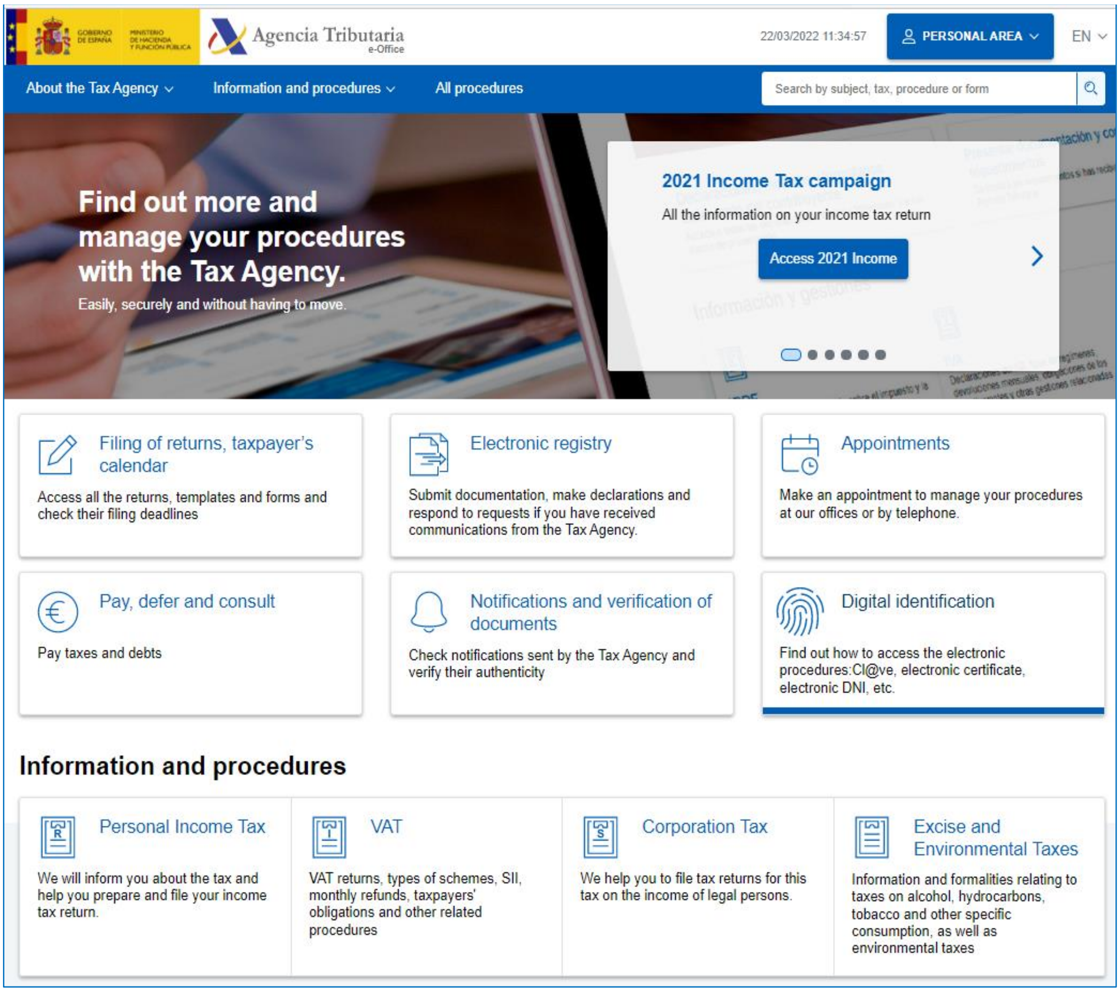
1. *Through the Internet without electronic certificate* - *Basic Level Registration*. If you do not have an electronic certificate, you can register online, requesting the invitation letter to the Spanish Tax Agency (AEAT), which will be sent by postal mail to your tax address, and completing the registration with the Secure Verification Code (CSV) that appears in the letter. Once we have the invitation letter we can complete the registration in the Cl@ve System. It should be noted that registration over the Internet without an electronic certificate will not allow access to certain services or use Cl@ve Signature.
2. *Through the Internet with electronic certificate or DNIe - Registration Advanced Level*. Citizens having a certificate or electronic DNI can register in the Cl@ve system through the Internet.
3. *In person at a Registration Office - Registration Advanced Level*. For the face-to-face registration in Cl@ve the physical presence of the person to whom it is to be registered will be essential.

Although initially the network of offices of the State Tax Administration Agency and the Management Entities and Common Services of the Social Security function as Registry Offices, the network of Registry Offices is expanded with those public bodies that have territorial deployment and meet the necessary technical requirements established.

The Spanish Tax Agency (AEAT) invitation letters are personalised and include a secure verification code (CSV) that can be used to register in the Cl@ve PIN system. They invite you to register at offices (maximum security level) or register on the AEAT website at Cl@ve-PIN, which is intermediate level, but is valid for the vast majority of AEAT procedures, following the criteria of proportionality in the use of different identification systems.

Figure A A.11. Unlocking services

Offering Digital Identification Options



Find out more and manage your procedures with the Tax Agency.

Easily, securely and without having to move.

2021 Income Tax campaign

All the information on your income tax return

Filing of returns, taxpayer's calendar

Access all the returns, templates and forms and check their filing deadlines

Electronic registry

Submit documentation, make declarations and respond to requests if you have received communications from the Tax Agency.

Appointments

Make an appointment to manage your procedures at our offices or by telephone.

Pay, defer and consult

Pay taxes and debts

Notifications and verification of documents

Check notifications sent by the Tax Agency and verify their authenticity

Digital identification

Find out how to access the electronic procedures:Cl@ve, electronic certificate, electronic DNI, etc.

Information and procedures

Personal Income Tax

We will inform you about the tax and help you prepare and file your income tax return.

VAT

VAT returns, types of schemes, SII, monthly refunds, taxpayers' obligations and other related procedures

Corporation Tax

We help you to file tax returns for this tax on the income of legal persons.

Excise and Environmental Taxes

Information and formalities relating to taxes on alcohol, hydrocarbons, tobacco and other specific consumption, as well as environmental taxes

Source: Spanish Tax Agency.

Next steps

The Spanish Tax Agency intends to evolve the AEAT Cl@ve PIN app to the Cl@ve app (Whole of Government) to make it a single point where we can offer citizens all the services related to means of identification, authentication and signature for the citizen of the Cl@ve platform. The development will be based on the Cl@ve PIN app, which is currently activated by 7 million citizens. In this way, the experience acquired in its development is taken advantage of and, in addition, the current user base will only have to migrate to the new app to have access to the new services that are offered. This evolution is again supported by the use of the mobile device as an element that all citizens (or practically all citizens) have and their capabilities to offer the two-factor authentication guarantees that are required to facilitate authentication. Substantial level according to eIDAS.

Challenges and lessons learned

There are a number of challenges currently being faced. These include, but not limited, to:

Adequate identification

The management of the health crisis situation caused by COVID-19 has illustrated the need for a new approach in taxpayer assistance and particularly in the classic Income Campaign, where in person, in our offices and in other collaborating entities, millions of income statements are prepared every year. The face-to-face attention was replaced by the telephone assistance, which, in addition to the challenge to be able to give a good service to the taxpayers, also represents a challenge to guarantee the adequate identification of the taxpayers to whom the assistance for the presentation of their Income Tax return will be facilitated.

Digital capabilities

It is necessary to carry out permanent training campaigns to obtain sufficient digital knowledge to operate the digital identity.

Implementing European eIDAS framework

A major challenge is to be able to offer cross-border digital identity services, and make sure that citizens of other countries can use Cl@ve through solutions such as the standard defined by the European eIDAS regulation, which allows the mutual recognition of electronic identities in the European Union. Perhaps the most important problem is how to distinguish taxpayers from countries that do not have a tax identification number at source.

United States

Domestic context

At present, the United States (US) does not have a universal, standardised digital identity (DI) program in place. Citizens are verified using various forms of identification such as a driver's license, passport, or other documents.

The US government began an initiative called the National Institute of Trusted Identities in Cybersecurity (NSTIC) in April of 2011 to improve the privacy, security and convenience of sensitive online transactions through collaborative efforts with the private sector, advocacy groups, government agencies, and other organisations. This helped lead to the creation and development of a public sector CSP that can be used in a federated model across any federal agency.

The public sector CSP as well as all future CSPs (public and commercial) have worked to align themselves against NIST SP 800-63 guidelines to support digital identities for any user population. These guidelines are continually reassessed and expanded upon due to the constantly evolving landscape around digital identity. SP 800-63-3 is in the process of being updated to a revision 4, due out in the first quarter of fiscal year 2023. As part of its revision process, NIST holds discussions with the public around specific areas being considered for revision. As part of those discussions, the IRS has worked closely with NIST (via monthly calls) to provide feedback for consideration for revision 4.

The IRS's Secure Access Digital Identity (SADI) program addresses the IRS's need to conform with National Institute of Standards and Technology (NIST) Special Publication (SP) 800-63-3. SADI leverages modern tools with the goal of providing a seamless and secure user experience for taxpayers accessing IRS online services.

The creation of digital identities will allow users to interact across multiple federal agencies leveraging a single DI; eliminating the need for multiple credentials. Additionally, the use of a DI will allow for non-US citizens, or US citizens living abroad to be able to access Internal Revenue Service (IRS) services regardless of their geographic location. This includes being able to verify non-US citizens with foreign identity documentation. The ability to identify/verify identities via trusted credential service providers (CSP) also support a user population that is often overlooked and underserved in the US. The types of evidence used to verify an individual have increased/improved allowing the underserved populations to be able to create a DI via CSPs to be able to access IRS services.

Current digital identity management system

The Internal Revenue Service (IRS) has been managing and maintaining multiple authentication and identity verification portals for various services it offers to the US taxpayer user population. As a result, users were required to create and manage multiple credentials depending on the services they needed access to. In order to provide a more streamlined, modernised authentication and identification verification process, and improve user experience, the IRS implemented a new Single Sign-On (SSO) portal that provides a single point of entry for authentication as well as a means for creating a single digital identity (DI) that may be leveraged within the IRS as well as across other federal agencies at a federal level. This implementation went live (into production) in the summer of 2021. The target audience for DI is for both individual and entity taxpayers, with initial focus on the individual taxpayer.

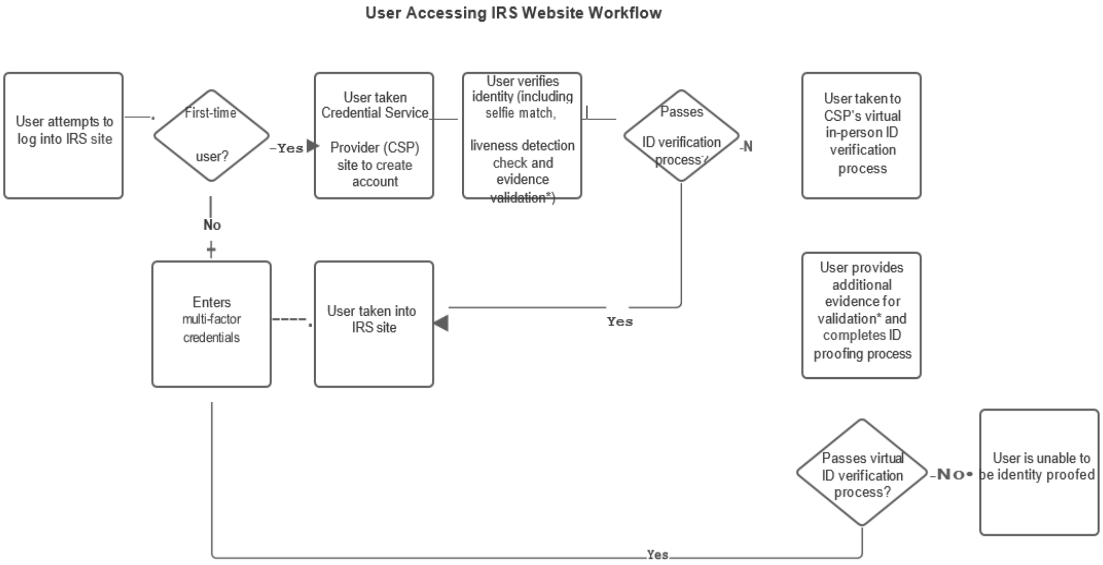
As part of this SSO portal strategy, the IRS does not identity proof and provide or manage credentials for taxpayers themselves. Instead, the IRS integrated with a commercial credential service provider (CSP) as well as a public sector CSP in order to provide users with more than one option for account creation and identity proofing services, and a single point of authentication via SSO. This integration also removes the burden of managing, maintaining, or supporting any end user related issues around DIs on the IRS as a whole; with both CSPs serving to create, manage, and maintain users' digital identities instead. By the end of 2021, there are over 4 million identities that have been successfully created and verified since the CSP integrations have been in production. Additionally, over an estimated 400 000 unsuccessful fraudulent user account creation attempts have been prevented by the CSPs.

Implementation

The SSO implementation required the build out of a new authentication portal to allow users to create an account and complete identity proofing/verification prior to being eligible to receive services. This included the planning, coordination, development, testing, and release of the CSP integrations. The IRS worked to communicate and socialise the new process for being able to access specific IRS applications, including new account creation process and identity proofing in advance of the CSP integrations and provided support after the initial launch to ensure that Americans would be able to access IRS applications seamlessly. One of the first applications to integrate with the SSO portal was to support Americans eligible for additional financial assistance as part of the American Rescue Plan, by allowing them to create a DI remotely and then accessing the Advance Child Tax Credit (ACTC) services.

Since its initial launch, the focus of the SSO portal has expanded to support other existing IRS applications that would benefit from an improved user experience in account creation and identity proofing/verification process prior to accessing IRS applications. The IRS is looking to migrate these applications behind the new SSO portal beginning fall of 2021 and beyond to offer a single point of entry for authentication, reducing the need for multiple authentication portals, which would also help reduce overall operational costs to the IRS.

Figure A A.12. User Accessing IRS Website Workflow


User Accessing IRS Website Workflow
User attempts to log into IRS site
First-time user?
Yes
User taken Credential Service Provider (CSP) site to create account
User verifies identity (including selfie match, liveness detection check and evidence validation*)
Passes ID verification process?
N
User taken to CSP's virtual in-person ID verification process
No
Enters multi-factor credentials
User taken into IRS site
Yes
User provides additional evidence for validation* and completes ID proofing process
Passes virtual ID verification process?
No
User is unable to be identity proofed
Yes

Source: Project Country Case Study US.

ID verification and account creation

The CSP account creation process at a high-level entails providing personally identifiable information that is verified against various authoritative sources; including biometric verification (e.g., selfie, liveness check); as well as documentation (aligned with NIST SP 800-63A guidelines) submission for verification. The verification process looks at "weighted" evidence based on NIST guidelines. These types of evidence are weighted as “Superior,” “Strong,” or “Fair” in strength. The different evidence provided depending on its strength determines whether a person can be successfully verified. Per NIST, an identity may be verified by one of the following combinations: 1. One piece of “Superior” evidence, 2. Two pieces of “Strong” evidence, or 3. One piece of “Strong” evidence and two pieces of “Fair” evidence.

The IRS is working with the CSPs to help define the various exception processes that are needed to support those that may be unable to create a credential via the standard online process, including accommodations for in-person or virtual in-person verification process, as well as accessibility requirements for information and communication technology (ICT) per Section 508 of the Rehabilitation Act. The IRS also works with tax practitioners who support individual and entity taxpayers, acting on their behalf.

The IRS engages with other federal agencies to support individual taxpayers, as tax administration account information is required to receive services from different agencies. The engagement between various agencies also allows for collaboration to share in integration processes, lessons learned, industry best practices, etc. across agencies.

By integrating with both a commercial and a public sector CSP at the IRS, users may leverage their single DI across other federal agencies that have also integrated with the same commercial and public sector CSPs, reducing the need for managing and maintaining multiple credentials and an improved overall user experience. This also provides users with more than one CSP option to create an account with. Ongoing research is being conducted to see how other organisations such as financial institutions may be used to assist with creating and verifying users’ identities.

Challenges and lessons learned

There are a number of challenges currently being faced. These include, but not limited, to:

Inclusiveness

The IRS has collaborated with other federal agencies to better understand the user populations that need to be supported, including those in the underserved population that may have a difficult time creating a digital identity. It also continues to collaborate with NIST to ensure that its solution is aligned with industry standards and best practices around security and privacy controls for information systems. Additionally, the IRS looked for ways that would facilitate users being able to access IRS resources the most efficiently; including exception processes for those needing accommodations such as accessibility, those unable to access IRS online due to lack of internet access, or even those with technological challenges such as digital literacy.

Security

The US continues to face a growing need to be able to easily and securely identify proof individuals online, either remotely or virtually which has become even more apparent due to the COVID-19 pandemic. With the US not having a mandatory national ID program in place, Americans continue to rely on paper or plastic-based identity credentials which were not designed to be easily validated online. Schemes involving synthetic have become more common, where fraudsters create accounts under fictitious identities in an attempt to exploit identity systems. Additionally, large company breaches have also contributed to the rise in identity theft overall. Concerns around data privacy and how that information is being used and stored, e.g., biometrics, also contribute to a form of mistrust that needs to be regained by the US government and the private sector.

The US government continues to support and augment existing public-private sector efforts by working with industry to set and define rules, identify sources of attributes controlled by industry, and establish parameters and trust models for validating and using those industry defined attributes.

Adoption

COVID-19 has accelerated the process in determining the need to create a means for individuals to be able to access IRS services remotely, more efficiently, and securely. Since the SSO portal has been in production (live), there have been over 4 million new accounts that have been successfully created via CSPs to access IRS services, and the IRS expects that number to continue to grow. The IRS continues to evaluate new and emerging technologies to see where the agency may align or benefit from the research being conducted.

References

OECD (2021), *G20 Collection of Digital Identity Practices: Report for the G20 Digital Economy Tak Force, Trieste, Italy, August 2021*, OECD Publishing, Paris, https://doi.org/10.1787/75223806-en. [5]

OECD (2017), *Shining Light on the Shadow Economy: Opportunities and threats*, OECD, Paris, https://www.oecd.org/tax/forum-on-tax-administration/publications-and-products/shining-light-on-the-shadow-economy-opportunities-and-threats.htm (accessed on 3 August 2022). [6]

Annex B. Taxpayer Identification in Cross-Border Situations

Trustworthy, and seamless cross-border identification is to the interest of all parties involved in taxation processes. Interests relate to service levels, compliance risks and administrative burdens and address questions like:

- How can taxpayers and their representatives seamlessly orchestrate taxation processes that relate to multiple tax administrations, preventing double or non-taxation?
- How can tax administrations support international business processes without introducing unnecessary burdens for both taxpayers, their representatives and administrations?
- How can tax administrations benefit from each other's identification management systems and how to establish mutually trusted systems and mechanisms?

This Annex presents nine use cases which for different groups of taxpayers and different tax types illustrate and detail these interests and challenges.[1] **To note, though, that these examples, produced by the administrations which led on this report, should be treated as illustrative since they may not represent the situation in all jurisdictions and, in some cases, practical aspects may be capable of being resolved by policy changes.** Further work on the identification of issues arising, including with business representatives, would be highly useful. (For that purpose a draft template has been developed in Annex C.) The generic issues identified for taxpayers, tax administrations and third parties not operating in federated systems (such as the EU) are set out in Chapter 2.

i) Tax administration services to non-residents without a physical presence, but taxable activity in the host country

An increasing number of individuals need to have access to services from a tax administration in another (host) country without having a physical presence there. The typical situation can be:

- a potential taxpayer owning properties and other assets that needs registration in the host country, or for instance taxable income for rentals, or being an expat,
- a representative for a company, trust or organisation with some kind of activity abroad that makes that individual responsible to interact with the tax authorities (and other government bodies) on behalf of that entity.

Digital IDs issued to a person with no presence are likely to reflect a lower trust level. By consequence, digital service quality levels will be reduced or may not even be delivered in a digital manner at all.

[1] These global use cases have been prepared together with tax administration representatives from the project's Advisory and Drafting Group.

Box B.1. Tax administration services to non-residents without a physical presence

Process description Use case 1

The steps below may vary dependent on type of service and the regulation in each country. The process is triggered by an individual's need to legally operate in the other country as a taxpayer or a representative.

1. The taxpayer contacts government to get information about the rules the government has for that particular registration and gets it as downloadable forms.
2. The taxpayer files the registration form and adds a copy of a passport and other necessary documents and files the documents to the (tax) authority.
3. The (tax) authority in the host country checks the ID and the other paper documents and issues an id number (if necessary) that makes it possible to register the individual in their IT-systems.
4. The tax authorities issue a digital ID (in most cases with limited access to services)
5. The taxpayer starts using available digital services; and paper based services for all other interactions.

Source: Project Global Use Case Template

ii) Temporary foreign subcontractors

This use case relates to foreign subcontractors with employees working in another (host) country, typically for a limited period of time, and where business registration and tax liabilities for different tax types are required in the host country. The interaction between these foreign businesses and the (tax) authorities in the host countries is not as seamless as in a domestic setting, which to a large extent is due to lack of trusted cross-border ID solutions.

Box B.2. Temporary foreign subcontractors

Process description Use case 2

The steps below may vary dependent on sectors, volume and countries. The process is triggered by a domestic (main) contractor and a foreign subcontractor signing an agreement.

1. The domestic contractor reports value and content of the contract with the foreign subcontractor to the tax authorities in the host country.
2. Foreign subcontractor registers as an entity in the host country and reports the contract to the tax authorities in the host country for tax registration, clarifying its tax status, identifying foreign employees working on the contract on behalf of the subcontractor, and submitting related (foreign) ID numbers and copies of ID documents, permits etc.
3. Tax administration in the host country registers employees and representatives for the foreign company in their computer systems.
4. Employees of the subcontractor undergo an ID-check of ID-documents to receive their domestic temporary ID-numbers when arriving – or after arriving- at the border. National (host country)

ID cards and/or digital identities might be issued to employees in order to use public digital services.

5. Employees of the subcontractor interact with the tax authorities in the host country updating their tax status – for instance whether a simplified taxation regime for employees applies, or tax returns are still mandatory – depending on length of stay, amount of pay, etc., according to host country rules.
6. The subcontractors withhold tax for their employees and pay taxes according to tax statuses.
7. The foreign subcontractor files tax returns and pay taxes according to the tax liabilities in the host country.
8. The tax administration issues a tax receipt for their stay (simplified tax regime) or a prefilled tax return.

Source: Project Global Use Case Template

iii) Temporary foreign workers (individuals)

Temporary foreign workers is an important supplement to a national workforce in order to secure the right capacity, knowledge and skills for a shorter or longer period of time. Each country has different regulations determining the nature of the workforce permitted into the country. The necessary process for government, is in many countries heavily paper-based and cannot be done before the immigrant enters the country. This is due to the inability to establish trust in the new digital ID in the host country and the inability to accept the digital ID from the country of origin.

Box B.3. Temporary foreign workers

Process description Use case 3

The steps below may vary dependent on sectors, volume and countries. The process is triggered by an invitation/confirmed contract from an employer in the host country. The steps or the order may differ from country to country, especially steps 4-6.

1. The immigrant applies for a work permit/visa based on the invite from the employer (digitally or on paper, submits copies of ID-documents/passports, id numbers from the host country).
2. The immigration authorities in the host country verifies the application and issues a work permit/visa.
3. The immigrant arrives in the new country.
4. The authorities conduct a verification process of id-documents of the person and issues an identification number for registration in government systems.
5. The immigrant interacts with the tax authorities to establish his tax status based on time of contract, amount etc. (simplified PAYE withholding tax or PAYE with a prefilled tax return).
6. If the immigrant meets the necessary criteria in the host country a new (digital) identity is issued in the host country.
7. The employer in the host country withholds personal income tax at the rate determined by the immigrant’s tax status.
8. The tax administration issues a tax receipt to the work immigrant for tax paid during the stay (simplified tax regime) or a prefilled tax return.

Source: Project Global Use Case Template.

iv) Selling goods to private individuals through electronic marketplaces and other digital platforms

Electronic marketplaces and other digital platforms such as Amazon, Alibaba, Rakuten or eBay play a critical role in the growth of e-commerce globally, including in online sales of consumer goods to private individuals.. These digital platforms allow businesses, particularly smaller businesses, to efficiently access millions of consumers in what has become a global marketplace. While these platforms' business models vary considerably and continue to evolve, e-commerce marketplaces will often take on a key role in facilitating and processing the transactions that are carried out through their platform. This typically includes controlling and/or setting the terms and conditions of the underlying transactions (e.g. price setting; payment terms; delivery conditions, etc.) and imposing these on participants (buyers, sellers, transporters etc.); direct or indirect involvement in payments processing; direct or indirect involvement in the delivery process and/or in the fulfilment of the supply; providing customer support services (e.g. product returns and refunds). The businesses selling through such digital platforms will generally be subject to taxation in their residence country. VAT on the sale of the goods is generally levied, if applicable, in the country where these goods are delivered. Goods that are imported from abroad as a result of the online sale through the digital platform may be subject to VAT at importation, via the normal customs procedure, although many jurisdictions apply an exemption from VAT for imports of goods with a value below the de minimis customs threshold as the administrative costs associated with collecting the VAT on the goods may outweigh the VAT that would be paid on those goods. In response to the continuous growth of cross-border e-commerce, a growing number of jurisdictions have legislated to make the digital platforms liable for the collection and payment of the VAT on the sales of goods that they facilitate, instead of the underlying suppliers (e.g. Australia, EU Member States, New Zealand, Norway, UK). This approach, which is in accordance with OECD standards and guidance, enhances the efficiency of VAT collection on online sales and allows tax authorities to focus their audit and enforcement efforts on a relatively small group of digital platforms rather than on the large numbers of underlying vendors that sell through these platforms. The collection of VAT on the commercial importation of goods (business-to-business transactions) is generally subject to a different regime than imports in a business-to-consumer (B2C) context. This may include an obligation for the importing business to declare the import VAT in its normal VAT return. Trustworthy and easily accessible cross-border identification of the parties involved in these transactions, including the platform operators and the underlying online sellers, is likely to further enhance the efficiency of tax compliance and administration and to strengthen tax authorities audit and enforcement capacity both in the home and host countries.

Box B.4. Selling goods through international platforms

Process example for sales to private individuals - Use case 4

1. The online vendor of consumer goods signs up to an e-commerce platform by registering among others: ownership, address, registration number/TIN number of the company, warehouse location, and country of origin.
2. The platform facilitates the presentation of the goods in its web store.
3. Customers, which may be non-residents, order on the platform. The customers pay for their online purchase by debit/credit card via a click-through on the platform.
4. The platform collects sales orders and payments and directs these to the sellers' systems.
5. The online vendor, digitally supported by the platform, records its sales and administers its accounts according to tax rules in its home country.

6. Transportation intermediaries (e.g. express courier or postal services) ensure the delivery of the items and ships these to the customer.
7. Where the goods are imported from abroad, and the digital platform is not liable for the VAT on the sales of the goods it has facilitated, any import VAT due will normally be collected through the traditional customs process. The customs authorities may require transport intermediaries (express couriers, postal services) to collect the VAT on the imported goods from the private customers, along with any additional fees.
8. The online vendor reports the transaction as part of its reporting requirements to the tax authorities in its home country.

Source: Project Global Use Case Template.

v) Selling services through sharing and gig economy platforms

The rise of the so-called sharing and gig economy (also known as the "collaborative economy") in recent years has been remarkable at both global and regional level. It has been powered by the growing capacity of digital platforms to connect millions of economic actors with customers worldwide. The sharing and gig economy involves large numbers of new economic operators, often private individuals, who monetise underutilised goods and services by making them available for temporary ("shared") use to primarily private consumers, via digital platforms. The growth of sharing and gig economy activity has created a new commercial reality in a number of industries, particularly in the sectors of transportation (with the emergence of "ride-sourcing") and accommodation (particularly in short-term rentals) and is also progressively transforming the professional services and finance sectors.. The "new ways of doing things" in the sharing and gig economy have raised questions whether existing tax frameworks are sufficiently equipped to capture this new economic reality efficiently, notably to protect tax revenues and minimise economic distortions between sharing and gig economy operators and traditional businesses. It also raises the question whether this new phenomenon, not least the role of sharing and gig economy platforms, creates new opportunities to enhance compliance and administration, and in particular, to help reduce the size of the informal economy.. At the core of these challenges is to ensure that tax administrations and platforms hold accurate data on the identity of taxpayers and their tax residence across, sometimes multiple, platforms and across borders. Without this, it is difficult for data on the identity of taxpayers to be transmitted securely between platforms and administrations.

Box B.5. Selling services through sharing and gig economy platforms

Process description Use case 5

1. The taxpayer registers on a platform from which they wish to provide services.
2. The platform requires proof of identity of the taxpayer as part of their own on boarding processes.
3. The taxpayer then provides services through the platform, and keeps necessary accounts for documentation.
4. The taxpayer completes their filing obligations and pays the required amount to the tax administration.
5. The tax administration audits the taxpayer's file.

6. The tax administration takes any necessary compliance action necessary, which may involve requesting information from the sales platform.
7. As the platform may be outside of the tax administration's jurisdiction, this request may take long response times or be unfulfilled.

Source: Project Global Use Case Template.

vi) Taxing property rentals for properties owned in another country

As globalisation has progressed many taxpayers own properties abroad, typically vacation homes. Property rental to other tourists is a normal way of covering cost of the ownership. The main rule is that the country in which the property is located (the host country) has the right to tax the income from the property rental. Depending on bilateral/multilateral agreements the taxpayer might also pay to his home country for the rental income. To avoid double taxation the rentals must be reported to both countries - taxes paid to the host country can be refunded or deducted through the tax return in the home country. The compliance process is complex, especially when rental is not covered through agents or platforms. Compliance risk is high, especially for the host country. The use of platforms raises questions regards the (responsibility for) identity matching across borders.

Box B.6. Taxing property rentals for properties owned in another country

Process description Use case 6

The steps below may vary dependent on regulation in each country. The process is triggered by a taxpayer's need to comply with legal frameworks in the host country. We assume the property is already related to the taxpayer by an issued personal id-number connected to a property number in a public registry in the host country. This might also be a basis for property tax not covered in these steps.

1. If required by the host country, the taxpayer registers the property for rental at the host country tax authorities – and might get a rental / tax number.
2. The taxpayer could decide to register with an agent/platform using the correct identification numbers required for identification of taxable transactions in the host country.
3. The taxpayer or agent markets the property to prospect tenants/renters.
4. The taxpayer or agent makes agreements and collects payments for property rentals and keeps necessary accounts for documentation.
5. If required by the host country, the taxpayer or agent reports and pays withholding tax to the local tax authorities as specified by host country tax laws.
6. The taxpayer/agent delivers necessary documentation for final rental property tax returns to the host country.
7. The taxpayer applies for refund by tax authorities in his home country. Documentation only available on paper from the host country is necessary for the application.

Source: Project Global Use Case Template.

vii) Delivering electronic services to private customers abroad

The digital economy has increasingly allowed the delivery of electronic services and digital products (applications, streaming of videos and music, gaming…) by businesses from a remote location to consumers around the world without any direct or indirect physical presence of the supplier in the consumer’s jurisdiction. Such remote supplies of services and digital products present challenges to traditional VAT design.

Consider an example of an online supplier of streaming digital content such as movies and television shows. The supplies are made mainly to consumers who can access the digital content through their computers, mobile devices and televisions that are connected to the internet. If the supplier is resident in the same jurisdiction as its customers, it would be required to collect and remit that jurisdiction's VAT on the supplies. However, if the supplier is a non-resident in the consumer’s jurisdiction, issues may arise in the absence of proper VAT rules.

Where the customer of services or digital products acquired from abroad is a VAT registered business, the VAT on this purchase will normally be self-assessed by this business through its normal VAT return (“reverse charge”). Such a self-assessment regime is however ineffectual for the collection of VAT on services or digital products acquired by private customers from foreign suppliers. To address this issue, the OECD has developed internally agreed standards requiring foreign suppliers of such services and digital products to register for VAT in the country where their private customer has its usual residence and to remit the VAT on these supplies via an online portal (“simplified registration and compliance regime”). These standards have now been implemented by approximately 80 countries worldwide with very positive results.

A key VAT compliance requirement for businesses that supply online services and digital products, which are often digital platforms through which millions of small businesses (e.g. app developers) sell these online products to millions of consumers around the world, is to know the status (business or private consumer) and the usual residence of their customers. Several tax authorities have implemented the possibility for online suppliers to verify the status and location of their customers automatically, through an API, on the basis of these customers’ digital identity (comprising VAT registration number and/or TIN). This significantly enhances both the ease of compliance and overall compliance levels. It also boosts these tax authorities’’ audit and enforcement capacity. Considerable further work is required, however, enhance consistency across jurisdictions in the tax identification of both suppliers and customers in online trade in electronic services and digital products.

Box B.7. Delivering electronic services to private customers abroad

Process description Use case 7

The steps below may vary dependent on type of service and the regulation in each country and is dependent on the principle of sellers collecting the VAT. The process is triggered by a foreign service provider who wants to accept sales to end consumers abroad.

1. The foreign seller goes online to get information on how to comply with regulations in each country they want to sell electronic services to.
2. The foreign seller registers for VAT in each of the countries where its private customers have their usual residence. (They might take advantage of a regime for registering once [one stop shop] for all countries within the EU).

3. The private customer makes purchases, specifying its place of usual residence and its status (business or private consumer; in the absence of a VAT registration number, the customer will often be considered to be a private consumer).
4. The foreign seller keeps the accounts with details for each sale necessary to separate VAT amounts to the specific country in question.
5. The foreign seller reports and pays the VAT related to sales to each country for each specified time period by the tax administration.

Source: Project Global Use Case Template.

viii) Withholding tax and refunds related to dividends for foreign shareholders

Dividends in general are taxed at source at a standard rate (for instance 25%) in the host country where the company is registered. For a foreign shareholder, the final tax liability to the host country is normally less and is determined by the shareholders country of residence. Exact rates vary and depend on tax treaties between countries, or by multilateral agreements (for instance EU/EEA). To be taxed at a lower rate a shareholder must prove his tax status to the host country, either in advance so less tax is withheld, or seek refund from the host countries afterwards.

Both processes create burdens on all parties involved and include paper-based information proving among other things beneficiary ownership and country of residence for tax. Strong incentives to document residency in a country with beneficial refund rates make this process subject to fraud.

Box B.8. Withholding tax and refunds related to dividends for foreign shareholders

Process description Use case 8

The steps below may vary dependent on type of service and the regulation in each country. The process is triggered by an individual’s, legal person or other entity’s need to operate legally in the other country as a taxpayer or a representative.

1. The company or its security representative creates a tax status list for all shareholders with adjusted tax status.
2. The company or its custodian pays out dividends to the shareholders and pays tax to the tax authority in the host country based on each shareholder’s tax status.
3. The foreign shareholder – or a representative for one or more shareholder - applies for lower tax rates / refund based on documentation that contains i.e. documentation on identity of beneficial owners, proof of ownership, taxes paid and tax residence status.
4. The tax authorities assess the tax status based on documentation and independently checks to verify the documents.
5. Refund is paid out to the taxpayer.
6. The documented accepted tax status might be used in a new application for reduced withholding tax in consecutive years.

Source: Project Global Use Case Template.

ix) VAT refund to foreign businesses for costs not subject to VAT in the host country

A jurisdiction's VAT regime should in principle ensure that a foreign, non-resident business has the possibility to recover any input VAT incurred in the jurisdiction that it would have been able to recover if it were a VAT-registered business located in that jurisdiction. This is to avoid undue discrimination between domestic and foreign businesses, in accordance with the internationally adopted core principle of VAT neutrality in international trade. To achieve this objective, most modern VAT systems provide the possibility for foreign businesses to apply for a direct refund of local VAT incurred. Some jurisdictions require that the granting of a refund to foreign businesses be conditional upon similar relief being granted by the jurisdiction of the foreign business claimant (a reciprocity requirement).

VAT refunds can be particularly vulnerable to fraud, which can range from simple over-reporting of input VAT to organised criminal attacks on the VAT system involving fake activities, false invoices and "missing trader" fraud. This may lead a tax authority to systematically carry out verifications of refund claims before approving them, often leading to lengthy, time-consuming and labour-intensive processes. This may result in backlogs of refund requests and businesses facing cash-flow pressures and the cost of having to pre-finance potentially considerable amounts of refundable input VAT. Modern VAT administrations therefore generally address refund-related fraud as part of a broader VAT compliance strategy based on risk management principles. They may limit in-depth verification checks to high-risk claims and apply fast-track refund processing for businesses without any detectable history of non-compliance. Trustworthy seamless cross-border identification of businesses could considerably contribute to further increase the efficiency of such risk-based VAT refund management processes.

Box B.9. VAT refund to foreign businesses for costs not subject to VAT in the host country

Process description Use case 9

1. A company acquires services in the host country that are subject to VAT (e.g. warehousing services).
2. The company or its representative files a refund application to the host country's tax administration in accordance with the host country's rules and procedures (for instance the minimum amount of the refund claim, the delay within which a claim must be filed, the type of purchases for which the refund claim is made etc.). The application may have to include supporting documents such as invoices, certificate of commercial activity from the home country, letter of attorney etc...
3. The tax authorities in the host country process the application. This might involve contacting sellers in the host country to confirm invoices or authorities in the company's home country.
4. The tax authorities - if the application is accepted – makes the refunds to the company on a known bank account.

Source: Project Global Use Case Template.

Annex C. Global Use Case template

Example Use case 1 - Tax Administration services to non-residents with no presence, but taxable activity in the host country

Introduction: Global taxpayer identification challenges

Tax administrations all over the world are faced with challenges when trying to identify taxpayers in cross-border situations. The Forum on Tax Administration's (FTA) project group on Global Digital Identity is collecting and describing examples of such identification challenges, referred to as use cases. The use cases describe a process where actors respond to a request/trigger.

This note details one specific use case example. By answering the questions below you are helping to enhance the levels of detail and understanding of the process and challenges. The aim is to analyse their impact on the tax system's performance.

The project group will use the data you provide for internal analysis purposes. Eventual publication of these data will be subject to your administration's consent.

Overall description

An increasing number of individuals needs to have access to services from a Tax Administration in another (host) country without having a physical presence there. The typical situation is:

- as a potential taxpayer owning properties and other assets that needs registration in the country, or for instance taxable income for rentals, or being an expat.
- as a representative for a company, trust or organisation with some kind of activity abroad that makes that individual responsible to interact with the tax authorities (and other government bodies) on behalf of that entity.

Digital IDs issued to a person with no presence will have a lower trust level. Digital services will be reduced or may not even be delivered at all.

Tax Types of relevance in your country:

Personal Income Tax	□
Capital Gains Tax	□
Corporate Income Tax	□
Value Added Tax	□
Employer Tax	□
Social Security Tax	□

Process description

The steps below may vary dependent on type of service and the regulation in each country. The process is triggered by an individuals need to operate legally in the other country as a taxpayer or a representative.

- The taxpayer contacts government to get information about what rules government have for that particular registration and get it as downloadable forms.
- The taxpayer files in the registration and adds a copy of passport and other necessary documents and files the document to the (tax) authorities.
- The (tax) authorities in the host country checks the ID and the other paper documents and issues an id number (if necessary) that makes it possible to register the individual in their IT-systems.
- The tax authorities issue a digital ID (with limited access to services)
- The taxpayer starts using limited services. Paper based services for all other interactions.

Process related questions:		
Does the process description above deviate significantly from the one in your jurisdictions?	*Yes □*	*No□*
If yes, could you please describe in what way it deviates?		

Exploring the challenge: Service quality

Service quality for these taxpayers and representatives are often vastly reduced.

Service quality related questions:	
How many non-residential taxpayers do you have in your country with less or limited access to digital services compared to domestic taxpayers due to trusted digital ID? Both actual numbers and percentage are relevant.	
How / In what way does the service level for foreign tax payers or representatives differ from a domestic setting?	
Are there any country specific circumstances or recent development that affects service quality?	

Exploring the challenge: Compliance risks

Paper based services increases the problem of non- intended errors and non-compliance. ID- fraud can still happen even if denied access to digital services. Accepting higher risk with lower trust identities is a tradeoff for some governments.

Compliance risk related questions:	
How big do you estimate the problem to be in your country? (revenue impacts/tax gaps, number of taxpayers involved etc.?)	
Which percentage of the tax gap does this concern? Amounts?	
In what way is ID misuse part of compliance risks in this use case and how big do you estimate this problem to be?	

How important is the lack of sufficient digital identity solutions for private individuals and companies in this use case?	
Are there any national circumstances or recent developments that might adding/subtracting to the problem in your jurisdiction?	
Are there closely related compliance issues you would like to mention?	

Exploring the challenge: Taxpayer burdens

Paper based services vastly increases the burden on the taxpayer

Taxpayer burdens related questions:	
Could you quantify the taxpayer burdens connected this issue? Could you please try to specify these burdens as detailed as possible (e.g. which activity, time and/or money related, number of taxpayers concerned, additional support of tax service providers…).	
How much of this is directly connected to the lack of effective cross-border identification?	

Exploring the challenge: Tax administration burdens

Tax administration burdens are closely related to processing paper based forms from the taxpayers.

Tax administration burdens related questions:	
Which burdens are caused by the cross-border identification challenges?	
Could you please try to specify these burdens as detailed as possible (e.g. which activities, time and/or money related, number of staff involved..)	
Do you have specific dedicated staff, teams, IT solutions, whole of government initiatives to deal with the challenge?	

General issues

Final generic questions:	
What is the core cause to the issue described above?	
Are you aware of any related cross-border taxpayer identification issues in this area that your tax administration (department) is facing?	

Annex D. Digital Transformation Maturity Model

Digital Identity	Emerging	Progressing	Established	Leading	Aspirational
Descriptor Indicative Attributes	*Identity as a taxpayer is established by the tax administration through the verification of documentary evidence. A TIN is created to identify the taxpayer for internal tax administration processes which remain largely within silos. There are very limited options for self-service although electronic submission of forms is increasingly possible.*	*For the majority of taxpayers, the administration creates basic digital identities which include TINs as attributes. Taxpayers are provided with credentials (often TIN and a password) which enables access to basic self-service options and communications between the administration and taxpayer, including online filing and payment. The administration is using TIN's to improve the digital joining-up of data within the administration as well as engaging with other parts of government on data sharing options.*	*More complex digital identities are created by tax administrations to access online services. TIN and password are no longer the only attributes to authenticate taxpayers as an increasing range of attributes are combined to create a more secure access to the digital identity allowing the administration to provide more self-service options. Digital identity has become a key enabler of joined-up tax administration and governmental processes and taxpayer self-service.*	*Individuals can use their digital identity to unlock services in different roles and (business) contexts. There is a shared digital identity vision across government as well as increasing collaboration with private sector partners. Digital identity supports a wide range of public/private service delivery and exchange of data. While the tax administration still centralises some data, increasingly taxation processes are built into some taxpayers' natural systems, making transactions more convenient and increasingly seamless, enabled by secure digital identity.*	*Whole of society digital identity is being developed and implemented allowing for comprehensive joining-up across the public and private sector. Digital identity supports taxation processes, including secure (near) real-time tax accounts, which are embedded into taxpayers' natural systems. The digital identity system is designed to facilitate international interoperability, supporting seamless usage of a digital identity in different public/private contexts and responsibilities.*
Creation of digital identity and the unlocking of service options.	Taxpayer registration and issuance of a TIN is generally done on a reactive basis following submission of appropriate forms and proof of identity by the taxpayer. Registration forms are available in printed format, although some forms may be available for	Identification for some taxpayers is increasingly supported by sending scanned identification documents, but still requires a degree of manual checking of documents within the administration. Individuals and entities are increasingly	Taxpayer registration and the creation of a digital identity is generally a digitised process for individuals in employment and is increasingly a condition of business registration. The administration engages with online platforms, trade associations and	Digital identities created by other government agencies, which may be triggered by other life events, can be used for tax purposes by the administration. Taxpayer registration is increasingly carried out seamlessly for most taxpayers, for	Digital identity system gradually facilitates the creation of an entire ecosystem offering a suite of identity services (e.g. authentication, retrieval of information, electronic signature). As whole of society digital identity develops, a whole of

Digital Identity	Emerging	Progressing	Established	Leading	Aspirational
	download on the administration's website. Registration is usually done in person or by mail, although for some classes of taxpayers online registration may be possible. A Tax Identification Number (TIN) may take a number of days to issue. TINs are generally used only in tax administration processes and communications and different identification numbers are used across government and the private sector	prompted and guided to register for tax following certain trigger events, such as registration as a business or for employment. Taxpayers are increasingly issued with a TIN and password on the same day. Engagement is starting with other parts of government on how and where government registration processes and issuing (and use) of identification numbers can be more joined-up (for example through the use of common data bases or linkages between existing registers)	other parts of government on the promotion and prompting of tax registration. Verification of electronic documents and issuance of a digital identity is possible in near to real-time. Enrollment processes for digital identities are increasingly joined-up across government agencies, bringing together government held information, for example population registers, passports or social security records through digitised processes within a legal framework.	example, when they first undertake taxable transactions, enter employment, register a business, or enter the jurisdiction for work purposes. The tax administration is fully engaged with the development and implementation of a strategy for whole-of-government digital identities, which is a key enabler to allow for an array of digital interactions between taxpayers and tax administration as well as third-parties (e.g. financial intermediaries).	government digital identity system is in place allowing taxation processes to be built into taxpayer's natural systems. This digital identity (or compatible digital identities) can also be harnessed by approved private sector organisations and is capable of working seamlessly across borders where counterparts have adopted internationally compatible digital identity standards.
	Most interactions with the tax administration remain paper based and, depending on the degree of risk of fraud, may require the submission of further proof of identity, for example through the sending of witnessed documents or presentation of credentials at the tax office.	Some digital services can be accessed by using TIN's and passwords although these are generally limited to submission of information to the tax administration. More risky processes, such as requests for refunds, change of personal details and delegation of authority cannot be carried out online. Delegation to carry out actions on behalf of the taxpayer can be authorised through online application processes.	The TIN and password is no longer a single digital identifier and a wider set of attributes (connected identifiers, characteristics and credentials) are connected together to securely represent the digital identity of a person or entity. This enables a wide range of e-services to be accessed directly by taxpayers. Applications to delegate certain actions to real persons (e.g. relatives or tax practitioners) can increasingly be carried out online.	The attributes associated with digital identity can both be harnessed by trusted public and private organisations. These attributes include enhanced security measures, such as biometric information, and are transparent to taxpayers. A public/private control framework is established allowing taxpayers to manage their digital identities, including delegations to authorised representatives and the operators of natural systems.	Taxpayers have a high degree of control over their digital identity. This includes the ability to choose specific data to share from their digital profile, to verify their ID, authorise the sharing of data, including to update attributes in real-time, and securely transact more seamlessly. Taxpayers can easily switch (private and business) roles within the tax system, using the same personal digital ID. This societal secure digital ID enables the orchestration of societal processes into seamless customer experiences.

Uses of digital identity within the administration and by taxpayers	TINs are used to identify taxpayers within the different tax administration functions, although taxpayer data remains within silos in general. Data can be accessed from other functions on request using the TIN (which is the identifier used across the administration). This scattering of taxpayer information can lead to delays for the taxpayer, for example as regards refunds and closure of tax positions, as well as duplication of reporting in some cases.	TINs are increasingly used to join up individual taxpayer information across different administration functions, improving the efficiency of processing within the administration and helping to drive improvements in the use of analytics and compliance risk management. Not all systems are fully integrated, though, so there is not a single picture of a taxpayer available to all tax administration functions in real-time.	Taxpayer data linked by digital identity is immediately accessible to all tax administration functions (subject to any legal restrictions on use and internal controls on access to data). Digital IDs increasingly allow the links to be made between taxpayers when they are acting in different capacities (such as for themselves or on behalf of entities) and allows a fuller risk picture to be built based on connections to other taxpayers.	Digital IDs, which are used across an increasing number of government agencies and some private sector actors, allows for the bringing together of increasing amounts of tax relevant data within the administration, This data is increasingly available in real-time rather than following periodic reporting cycles. These integrated digital identity functions enable tax administrations to service taxpayers from a more holistic perspective.	The tax administration is fully embedded in a whole-of-society system of digital identity (whether unique or compatible digital identities). The tax administration has a real-time holistic picture of the taxpayer, taxable events and their natural system touch points This also allows the tax administration to adequately find, service and tax entities and persons abroad. Where taxation processes are built into taxpayers' natural systems, digital access is available to the tax administration for proactive, personalised, assurance processes, supported by the use of artificial intelligence.
	Some self-service offerings, which can be accessed through the TIN and an account password, are generally limited to viewing basic identity information about the taxpayer. The taxpayer is able to query the information electronically in some cases but is unable to amend it directly. The administration is starting to develop a strategy for the expansion of digital identification and self-service options for taxpayers.	Basic digital identification gives taxpayers access to a portal/platform allowing them to view personal information or notices from the administration and to increasingly interact digitally with the tax administration (for example reporting, payment and some verifications). Passwords to access the portal are sent by mail to the taxpayer's registered address and have to be used along with the TIN. For security reasons, limitations or exclusions are in place for some processes to be done in real-time	A wide range of digital taxpayer services, including for refunds and amendments of taxpayer information, can be unlocked by the use of digital identities and more secure authentication processes, such as multi-factor authentication. A legal framework is in place for allowing two way sharing of information across government and some private sector actors, but this is not yet fully operational due to lack of compatibility across digital IDs.	Digital identity supports taxation processes being embedded within some taxpayers' natural systems, in particular for elements of personal income tax and small business taxation, although the administration continues to centralise large amounts of data for the processing of tax liabilities and risk assessment. Taxpayers can use their digital IDs to access up-to-date information across many government and some private sector platforms. Taxpayers can increasingly use	Increasingly real-time taxation processes are embedded in taxpayers' natural systems for all taxpayers, with digital identity supporting the real-time exchange of information from all relevant parties necessary for such processing. Tax relevant data is sent from taxpayers' natural systems to the administration when taxable events occur allowing the taxpayer to have an up-to-date understanding of their current tax position. Overall, trust drives taxpayers' adoption

		such as changes of details, refunds or viewing of some records.		biometric and other authentication methods built into their natural systems	and use of joined-up/ integrated digital identity enabled services

OECD FORUM ON TAX ADMINISTRATION

Tax Administration 3.0 and the Digital Identification of Taxpayers

Initial Findings

The 2020 report ***Tax Administration 3.0: The Digital Transformation of Tax Administration*** identified effective digital identity as one of the core building blocks for enabling seamless tax administration as it can help provide a secure connection between the systems of tax administrations and taxpayers. This report, ***Tax Administration 3.0 and the Digital Identification of Taxpayers: Initial Findings*** explores the current state of play on digital identity, the different domestic solutions adopted in a number of jurisdictions as well as the challenges related to cross-border processes. It also lays the groundwork for future collaborative work with business and other stakeholders in this area. This report was developed by officials from Australia, Canada, Finland, Indonesia, Spain, Norway, the United States, and supported by the Secretariat for the Forum on Tax Administration.

www.oecd.org/tax/forum-on-tax-administration/