



OECD Digital Government Studies

# Digital Government in Chile – Digital Identity





OECD Digital Government Studies

# Digital Government in Chile – Digital Identity

This work is published under the responsibility of the Secretary-General of the OECD. The opinions expressed and arguments employed herein do not necessarily reflect the official views of OECD member countries.

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.

**Please cite this publication as:**

OECD (2019), *Digital Government in Chile – Digital Identity*, OECD Digital Government Studies, OECD Publishing, Paris, <https://doi.org/10.1787/9ecba35e-en>.

ISBN 978-92-64-90243-5 (print)  
ISBN 978-92-64-93885-4 (pdf)

OECD Digital Government Studies  
ISSN 2413-1954 (print)  
ISSN 2413-1962 (online)

The statistical data for Israel are supplied by and under the responsibility of the relevant Israeli authorities. The use of such data by the OECD is without prejudice to the status of the Golan Heights, East Jerusalem and Israeli settlements in the West Bank under the terms of international law.

**Photo credits:** Cover © Fundación Imagen de Chile.

Corrigenda to OECD publications may be found on line at: [www.oecd.org/about/publishing/corrigenda.htm](http://www.oecd.org/about/publishing/corrigenda.htm).

© OECD 2019

---

You can copy, download or print OECD content for your own use, and you can include excerpts from OECD publications, databases and multimedia products in your own documents, presentations, blogs, websites and teaching materials, provided that suitable acknowledgement of OECD as source and copyright owner is given. All requests for public or commercial use and translation rights should be submitted to [rights@oecd.org](mailto:rights@oecd.org). Requests for permission to photocopy portions of this material for public or commercial use shall be addressed directly to the Copyright Clearance Center (CCC) at [info@copyright.com](mailto:info@copyright.com) or the Centre français d'exploitation du droit de copie (CFC) at [contact@cfcopies.com](mailto:contact@cfcopies.com).

---

---

## Foreword

Governments around the world are struggling with establishing personal identity in a digital age, since policies and legal frameworks that combine physical and digital identification elements are complex to develop. *Digital Government in Chile – Digital Identity* aims to support the Government of Chile in designing effective and trustworthy identity management.

As requested by the Ministry General Secretariat of the Presidency (*Ministerio Secretaría General de la Presidencia*, MINSEGPRES) and the Ministry of Finance (*Ministerio de Hacienda*), the report discusses Chile's experience and benchmarks its performance against 13 OECD countries. The study is based on the OECD Recommendation of the Council on Digital Government Strategies and builds on the 2016 OECD report, *Digital Government in Chile: Strengthening the Institutional and Governance Framework*, which guided recent institutional reforms for digital government in Chile.

While Chile is a recognised digital government leader in Latin America, strong digital identity management will be critical for Chile to deliver effective digital government infrastructure and provide better services to its citizens.

This study also contributes to the global policy debate on the digitalisation challenges and opportunities across different policy areas, including digital government. This work is part of the Going Digital Project, which is the OECD flagship initiative designed to address this important policy issue.



---

## *Acknowledgements*

*Digital Government in Chile – Digital Identity* was prepared by the OECD Directorate for Public Governance (GOV), under the leadership of its Director, Marcos Bonturi.

The report was produced by the OECD Reform of Public Sector Division (GOV/RPS). It benefitted from the strategic orientation and revisions of Barbara-Chiara Ubaldi, Acting Head Division and lead of the Digital Government and Open Data Team.

The report was drafted by Benjamin Welby, Digital Government Policy Analyst, Reform of Public Sector Division, OECD; and Andrés Vasconcelos, digital government policy consultant. The authors are grateful to Liv Gaunt for editorial and administrative support.

The report benefitted from the expertise of the OECD Working Party of Senior Digital Government Officials (E-Leaders). This project would not have been possible without the support of the Chilean Ministry General Secretariat of the Presidency, the Ministry of Finance and its State Modernisation Programme.

Finally, the Secretariat would like to acknowledge the contributions of Andrés Bustamante, Head of the Digital Government Division of the Chilean Ministry General Secretariat of the Presidency, and Kareen Schramm, Policy and Digital Government Research Co-ordinator of the same institution. The OECD would also like to warmly thank Randall Ledermann and Felipe Gonzalez Zapata, Project Coordinators of the State Modernisation Programme, Ministry of Finance, Chile. Without their leadership and vision this project would not have been possible.

## *Table of Contents*

<b>Foreword</b> .....	<b>3</b>
<b>Acknowledgements</b> .....	<b>5</b>
<b>Executive summary</b> .....	<b>7</b>
<b>Assessment and recommendations</b> .....	<b>9</b>
Foundations for DI .....	9
DI solutions .....	12
Policy levers and adoption.....	14
Transparency and monitoring.....	18
<b>1. Introduction</b> .....	<b>21</b>
DI assessment framework.....	25
Note.....	26
<b>2. DI in selected countries</b> .....	<b>27</b>
Dimension 1: Foundations for DI.....	28
Dimension 2: DI Solutions .....	41
Dimension 3: Policy levers and adoption .....	54
Dimension 4: Transparency and monitoring .....	62
Observed trends.....	69
References .....	70
<b>3. DI in Chile</b> .....	<b>71</b>
DI in Chile.....	72
Foundations for DI in Chile.....	72
Chile’s technical DI solution .....	79
Policy levers and adoption.....	82
Transparency and monitoring.....	88
References .....	90



## *Executive summary*

The challenge of proving someone is who they claim to be, were born in a particular place, live at a certain address and have the legal standing to do business, cross borders, access medical care or go about life is an age old problem that has historically been dealt with by creating physical tokens. As the digital transformation of society changes expectations in the delivery of public services, and governments seek greater efficiency in response to budgetary constraints, there is an ambition to move away from face to face interactions towards digitally enabled solutions.

*Digital Government in Chile – Digital Identity* draws on the experience of 13 member and non-member countries (**Austria, Canada, Denmark, Estonia, India, Italy, Korea, New Zealand, Norway, Portugal, Spain, United Kingdom and Uruguay**) to establish an analytical framework for understanding how to develop and implement a digital identity (DI) approach that supports the transformation of government. The study aims to support the Government of Chile in enhancing their approach to DI as a piece of core digital government infrastructure and an enabler of improved service delivery. It uses a framework that covers the foundations for identity in terms of existing national identity infrastructure, policies and governance, technical solutions, the factors which impact adoption within the public sector and citizens, and the ways in which DI can create greater transparency of the working of government, and empower citizens through greater control of their data.

In providing concrete and actionable policy recommendations to underpin the effectiveness of DI efforts this study represents the third report completed by the OECD Secretariat to support the Government of Chile transition to a digital government. The Chilean Ministry General Secretariat of the Presidency (*Ministerio Secretaría General de la Presidencia*, MINSEGPRES) and the Chilean Ministry of Finance (*Ministerio de Hacienda*) have demonstrated the vision to build a government for the 21st century in working with the Secretariat to develop their approach first to the question of governance with the 2016 study *Digital Government in Chile: Strengthening the Institutional and Governance Framework*.

*Digital Government in Chile – Digital Identity* is complemented by the Study *Digital Government in Chile – Making the Digital Transformation Sustainable and Long-Lasting*, which looks at creating sustainable and strategic change, and a report that will focus on revamping Chile's service delivery strategy.

### **Key policy recommendations**

- Build Chile's DI on the existing infrastructure provided by the Civil Registry Service of Chile (*Servicio de Registro Civil e Identificación*, SRCeI) and the *Cédula de Identidad*. As a result Chile does not need to pursue the generation of validated identities with the private sector.
- Ensure the focus on DI within the Government's Digital Transformation Strategy is sustainable through the provision of long term financial and political commitment.
- Identify or create a senior responsible role with responsibility to shape and deliver identity according to the vision established by the Government's Digital Transformation Strategy.

- Consider the design of identity management (both physical and digital) as an end-to-end process throughout a citizen's life from birth, through life and at death. This should consider the future possibilities of technology in the physical identity card, creating the conditions to iterate the service, and ensure a clear understanding of the needs of users both within and outside government.
- Prioritise development of ClaveÚnica to support putting the citizen in control of their data and being able to grant, and revoke, permissions to access and use it.
- Reach an understanding of the identity needs for businesses and develop a shared roadmap with the relevant organisations for the future state of DI in general. This may need to include the convergence of business and citizen DI and the transition of users to consolidate usage around a single approach.
- Identify priority private sector services for the use of ClaveÚnica and establish a working partnership to ensure ClaveÚnica works for the private sector as well as the public sector.
- Establish the adequate legal and regulatory framework to manage the use of ClaveÚnica credentials to access private sector services, particularly where that opens the possibility of personal data being reused.
- Explore with regional partners how interoperability of identity can facilitate cross-border services and meets the needs of Chilean residents abroad.
- Use the expansion of ClaveÚnica as an opportunity to provide citizens with digital literacy and digital skills training through ChileAtiende and other face to face locations whilst people are activating their ClaveÚnica for the first time.
- Include DI as an explicit topic in spend controls, quality assurance processes, design guidelines and training and capacity building. This is to maximise awareness and adoption within government and avoid the development of duplicate solutions.
- Make funding available to meet the needs of government teams in seeing ClaveÚnica as a reliable and respected service. This should ensure the design of ClaveÚnica's technical solution is easy to implement and supported by ongoing reference materials, guidance and, where necessary, consultancy. It should also include the necessary support to service teams in producing clear cost-benefit analysis and rationale for identifying return on investment when making business cases for implementation and adoption.
- Review the mechanisms by which public agencies agree to exchange data and provide guidance and boilerplate templates to support a more efficient process. This should complement efforts to implement interoperability standards across both legacy and newly developed systems.
- Identify Key Performance Indicators relating to the time and cost involved in providing non-DI enabled services to provide a baseline for measuring, comparing and demonstrating the benefit of implementing DI. Publish this as Open Government Data and within the performance dashboards detailing the quality of service provision in Chile.

## Assessment and recommendations

Over recent years Chile has been working with the OECD to explore how they might maximise the potential of digital government to transform the relationship between the citizen and the state and improve the quality of public services. To seize that opportunity requires governments to undergo a transformation that starts from a shared vision and robust institutional frameworks that develop the State's capacity to implement such a strategy.

With the necessary governance in place, and a clear vision provided, specific enablers, such as Digital Identity (DI), become a greater priority. As countries look to develop services that can be accessed online and delivered through the more intelligent and proactive sharing and reuse of data across the public sector, it is essential that countries have a mechanism that validates and verifies that someone is who they say they are. Historically this has been made possible through the proofs and checks that take place through face to face contacts like signatures and physical tokens. Taking full advantage of the transformation which DI makes possible is about more than simply digitising those analogue interactions.

This *Digital Government Study* has analysed the experiences with DI of several OECD countries and provides insights for Chile in exploring how the Country develops and enhances its own approach to DI. It considered the necessary foundations for DI, the technologies that are used, the policy levers and constraints that shape DI's role in delivering public services and finally how the impact and performance of such activities can be better understood.

### Foundations for DI

#### *National identity infrastructure*

Chile has an important foundation in place for the future of DI in the Country. The existing *Cédula de Identidad* is a familiar piece of identity infrastructure backed by the Identification and Civil Registry Service of Chile (Servicio de Registro Civil e Identificación, SRCeI). This public sector provided identity is the necessary enabler to *ClaveÚnica* to simplify the identity landscape in Chile. It affords an opportunity to work with the private sector in delivering services rather than needing to explore a different model for generating validated identities.

Nevertheless, the interaction between this physical identity and any future DI should be considered as part of a single service design. This means that Chile should consider how to make the enrolment process for both the *Cédula de Identidad* and *ClaveÚnica* as easy as possible for their citizens. The current manual process for initial enrolment for a *Cédula de Identidad* is onerous for both the citizen and the government. In line with proactive thinking about how to deliver services before citizens recognise the need for interaction with the government, Chile should consider the design of identity management (both physical and digital) as an end to end process throughout a citizen's life from birth, through childhood, on into adult life and eventually at their death.

As Chile considers how its physical identity card can complement DI they should draw on the experiences of **Italy**, **Spain** and **Uruguay** in developing a contactless approach to accessing the information contained within the card. This will enable Chile to make use of NFC technology in smartphones and obviate the need for citizens and businesses to obtain devices specifically for reading cards.

### *DI policy*

The strategic role of ClaveÚnica has been recognised by President Pinera and Government's Digital Transformation Strategy. This commitment to its role in the future transformation of service delivery in Chile, and the subsequent high level of mandate that it provides, are essential in addressing internal obstacles to adoption. Whilst all further opportunities should be taken to reinforce this mandate, it is not sufficient by itself to ensure the quality of services or the ease of adoption.

Further political and financial support should be given to the SRCeI and Digital Government Division (DGD) to support the development of ClaveÚnica as a reliable and respected service within government and the private sector as much as for the public. This investment should include account management capability for managing and stimulating adoption, investment in technical documentation and simple on boarding to support internal colleagues and guidance on how to understand and define benefits for providing the return on investment.

Chile should consider the role of DI in the ongoing development of a more sophisticated and mature approach to the transformation of government services. The enabling technology of DI is an important element of any thinking about the design and content of assurance processes, capacity building and design guidelines. To support these efforts Chile should develop a renewed and comprehensive policy for DI that is ambitious for transforming government services and includes a roadmap for adoption and clear metrics to assess its impact.

DI should also form part of any analysis of spending for new government services to ensure that there is no competing investment in alternative DI solutions. Furthermore, Chile should ensure that the mandate provided to ClaveÚnica extends to retiring existing models of DI and leads to the development of an agreed roadmap for the delivery of functionality and the transition of users from established models into ClaveÚnica.

Finally, Chile should ensure that DI is recognised in the National Digital Security Strategy so that the necessary security operations activity is recognised and resourced to safeguard citizen data and those government services which use ClaveÚnica. A 2017 study into the reasons for citizen preferences for face-to-face interactions identified that the perception of security of transactions is a significant determining factor in the choices people make. As such, it is critical to coordinate with those responsible for the digital security strategy (MIDESO, 2017<sup>[1]</sup>).

### *Governance*

The management of ClaveÚnica and the associated activities for providing and establishing DI in Chile require strong governance arrangements and an ongoing political and financial commitment at both the centre of government and within individual public sector organisations to support successful adoption.

Although it is a strength for Chile's national identity infrastructure to be provided by SRCeI and for DGD to have a leading coordination role on digital transformation across the

Country, the separation of responsibility for identity from those responsible for the success of the digital transformation agenda could present risks to the success of efforts to implement DI in Chile and avoidance of duplication. Therefore, coordination and collaboration must be ensured between SRCeI and DGD with continuous monitoring by the Modernisation of the State committee. To support this the Government should identify or create a senior role whose responsibility it is to shape and deliver the implementation and operation of DI on the basis of the vision established by the Government's Digital Transformation Strategy. This senior role should be supported by an appropriate cross-government coordinating body including representation from the Ministry of Finance, the Ministry General Secretariat of the Presidency (MINSEGPRES), the Ministry of Justice and the Ministry of the Interior as well as representation from the Ministry of Economy to ensure the promotion of DI in the private sector as well. This may be incorporated into existing governance structures or, due to the importance and potential technical nuances of the subject, require the creation of something new.

Such a group would help Chile rationalise its existing DI landscape to ensure that the citizen experience can be as simple as possible. Whilst the Presidential Instruction on Digital Transformation is to be welcomed in establishing the initial guidelines for converging on a unique DI mechanism, *ClaveÚnica* currently competes with other institutional models of DI such as that provided by the Chilean tax office (*Servicio de Impuestos Internos, SII*). Having committed to convergence, it is now critical to implement the necessary governance and delivery arrangements for managing the roadmap for achieving this.

Alongside the mandate from senior political leaders and senior institutional leaders, the necessary support must be provided to teams within government to simplify and support adoption. This means not only providing a high quality technical solution but providing the necessary support and guidance that instils confidence in *ClaveÚnica* without needing to resort to governance arrangements that force compliance. This is especially important in the context of handling any convergence of existing DI mechanisms.

The final area of governance that Chile needs to establish relates to the future working relationship between the public and private sectors. With Chile prioritising the use of *ClaveÚnica*, backed by the *Cédula de Identidad*, it is most relevant for Chile to work with the private sector to establish a common purpose in delivering a DI solution which works for accessing services regardless of whether they are provided by the public or private sectors. It is less of a priority for Chile to work with the private sector to explore a marketplace of identity provision supplied by the private sector or to invest in using private sector identity to access government services.

Proposals for action	Level of Priority
In light of the preceding assessments, which draw on the analysis of the 'Foundations for DI', the Chilean government could consider implementing the following recommendations:	
Chile should build their DI on the existing infrastructure provided by the SRCel and the <i>Cédula de Identidad</i> . As a result Chile does not need to pursue the generation of validated identities with the private sector.	High
Although ClaveÚnica enjoys high profile political backing and forms a central part of the Government's Digital Transformation Strategy Chile should ensure that there is a long term financial and political commitment to ensure that it is able to establish itself within the provision of public and private services	High
The government should identify or create a senior role with the responsibility to shape and deliver identity on the basis of the vision established by the Government's Digital Transformation Strategy.	High
Chile should consider the design of identity management (both physical and digital) as an end to end process throughout a citizen's life from birth, through childhood, on into adult life and eventually at their death. This should include thinking about the future possibilities for contactless technology in the physical identity card.	Medium
Funding should be made available to SRCel and DGD to develop ClaveÚnica as a reliable and respected service within government. This investment should provide for account management, simple onboarding and support with identifying return on investment	High
Include DI as an explicit topic in spend controls, quality assurance processes, design guidelines and training and capacity building. This is to maximise awareness and adoption within government and avoid the development of duplicate solutions.	High
Chile should develop a plan for cataloguing and managing the different existing models of DI and where appropriate developing a roadmap for feature parity and a timeline for account transition and convergence	Low
Identify priority private sector services for the use of ClaveÚnica and establish a working partnership to ensure that the future of ClaveÚnica works for the private sector as well as the public sector	High
The National Digital Security Strategy should prioritise the necessary security operations to ensure ClaveÚnica is a safe and trusted identity platform	Medium

## DI solutions

Chile's current approach to DI provides a very straightforward authentication mechanism that works for online services that are accessed through the browser. The quality of that identity is robustly underpinned by the *Cédula de Identidad* and an increasing number of government services are confident in using it for delivering value to citizens. Chile should continue to build on the SRCel.

Indeed, the future vision for ClaveÚnica is significantly more sophisticated with the ambition to provide a suite of functionality to citizens including a data wallet and attribute exchange. The future plans for ClaveÚnica compare favourably with the ambitions and experiences of the countries surveyed in this study and Chile should be confident about progressing in that direction as it allows them to consider the transformation of services and redesign of the state rather than the more rudimentary like for like digitisation of existing analogue processes.

To support Chile in delivering a DI model that achieves the transformation of identity those involved with providing ClaveÚnica as a service should ensure they have a clear understanding of its users and their needs both within the provision of services and its implementation. For the public it is essential to simplify the experience of enrolment and usage to ensure it is easy to successfully use it. For colleagues within government steps need to be taken to facilitate the adoption of ClaveÚnica and the effective realisation of benefits.

An important characteristic of ClaveÚnica is its technical underpinnings. By being built on top of OpenID Connect, which is based on the Open ID and Open OAuth frameworks, the underlying architecture enables the simplicity enjoyed by private sector services that use forms of 'Bring Your Own Identity' to be applied to Chilean government services. The value of developing a straightforward technical solution can be seen in the speed with which ClaveÚnica has been adopted by government services in the last twelve months.

Although the way in which ClaveÚnica operates uses the *Cédula de Identidad* and its RUT as a means of second factor authentication, Chile should consider how the security of their DI model could be enhanced by implementing an SMS or Authentication app based confirmatory code when accessing services to ensure that the person accessing the service is the ClaveÚnica account holder. Chile should consider the role of mobile devices in supporting a simple approach to two-factor authentication rather than exploring smartcard approaches that may require the wholesale replacement of existing physical identity cards and the requirement for bespoke hardware either on an individual's computer or in accessing a service.

It is also important that Chile recognises the importance of developing DI solutions that meet the needs of businesses and legal persons. This may be covered by the anticipated signature and attribute exchange functionality of ClaveÚnica but it is critical that any solution also works in the context of the existing needs and experience of the Chilean tax office (SII) (*Servicio de Impuestos Internos*). It may be effective for Chile to consider coordinating the development of Clave Única with the needs of Chilean tax office (SII). . However, this does not need to be as high a priority for development as expanding the functionality of ClaveÚnica.

Although Chile's *Cédula de Identidad* contains biometric data, in the shape of a photograph and a record of the right thumbprint, this is not a feature of the DI experience in Chile. Furthermore, the surveyed countries demonstrated that the application of biometric information for validating the identity of a user is not yet a mainstreamed activity and one that can draw other challenges in terms of data protection and the trust of populations, as well as potentially incurring greater costs. As such, it is refreshing to see that Chile is focused on getting the basics of identity working in an effective way that establishes trust amongst the population through the development of consent models and tools to manage access. As Chile develops its understanding about the needs for elevated levels of identity verification, and implements more sophisticated digital services that require the authentication offered by biometric proofs, then these applications could be considered, but this is not a priority at this phase of the development of ClaveÚnica.

Proposals for action In light of the preceding assessments, which draw on the analysis of 'DI solutions', the Chilean government could consider implementing the following recommendations:	Level of Priority
Chile should commit to building ClaveÚnica on top of the Civil Registry and the existing physical identity infrastructure provided by the <i>Cédula de Identidad</i> .	High
Chile should ensure that the design of ClaveÚnica's technical solution is easy to implement and supported by ongoing reference materials, guidance and where necessary consultancy from the DGD/SRCeI development team	High
Develop an approach to two factor authentication that meets user needs	High
Developing ClaveÚnica along the lines of the stated future vision, especially in the areas of modelling consent, putting the citizen in control of their data and enabling the revocation of permissions should be a priority.	High
In designing and implementing the future version of ClaveÚnica with its expanded feature set, DGD/SRCeI should ensure that they have a clear understanding of the needs of users both within and outside government and be in a position to iterate the ClaveÚnica service offering accordingly	High
Over time, DGD and SRCeI should work with SII to reach a common understanding of the identity needs for businesses and develop a shared roadmap for the future state of DI in Chile. This may need to include the convergence of both citizen and business approaches, and transition of users from one DI solution to another.	Low
Consider the needs of biometric identity proofing when designing new services and explore how future iterations of ClaveÚnica can take advantage of this information making sure to balance the opportunities with the sensitivities of data protection and security	Low

## Policy levers and adoption

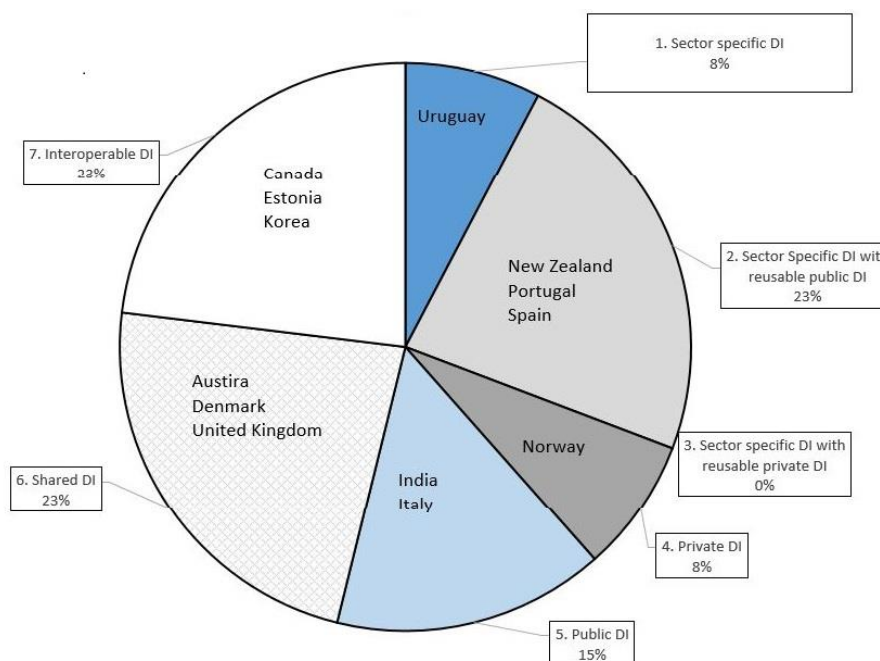
### *Legal and regulatory framework*

Efforts to stimulate adoption simply for the sake of adoption are less attractive than exploring those policy levers and enablers which will ensure that DI is useful and usable and which is consequently desirable to possess. With DI acting as an enabler of access to transformed government services its utility is found when there is a need for that interaction.

The Chilean government requires anyone over the age of 18 to have the *Cédula de Identidad* but there is no equivalent expectation for citizens to hold a ClaveÚnica account. Requiring citizens to be in possession of a DI is one way of encouraging adoption but introduces a level of compliance and enforcement. Nevertheless, the fact that ClaveÚnica is built on top of a physical identity infrastructure that has a legal requirement to be held means the country has a strong foundation for encouraging adoption of the DI even if citizens are not habitually accessing digital government services. Chile should explore how best to simplify the relationship between the identity card and the digital element so that the user experience of enrolling, managing and using the two are closer together. Legal changes may be required to reflect any requirement to be in possession of both.

Currently, different aspects of the arrangements for identity are handled between DGD and SRCeI. An approach where the responsibilities are shared in this way can work with the appropriate coordination arrangements but it may prove more effective in terms of transformation to unify the management and delivery of identity. This would mean no longer considering identity as two separate elements, physical and digital, but to consider them part of the same service design challenge with the same underlying and enabling policy and legislative frameworks.



**Figure 2.9. DI models found in selected countries**

*Source:* Based on information provided by Austria, Canada, Denmark, Estonia, India, Italy, Korea, New Zealand, Norway, Portugal, Spain, United Kingdom and Uruguay in response to the OECD survey Benchmarking Digital Identity Solutions (Unpublished).

As Chile explores the appropriate business model for the delivery of DI, decisions will be needed about the legal and regulatory framework for that model. With *ClaveÚnica* being built on top of the SRCeI this reduces the role of the private sector in providing identity. However, if it is decided to explore a different working arrangement with the private sector, perhaps to consider a shared model of identity provision as implemented in Austria, Denmark and the United Kingdom, then new legal and regulatory frameworks will be needed. Moreover, as there is an ambition for Chile's DI to be used in accessing services in the private and public sectors Chile may need to revisit its existing legal and regulatory provision for managing how private sector services consume and make use of *ClaveÚnica* and the data to which it grants access.

The successful implementation of DI removes one of the barriers to the data held by one part of government being accessed and reused by another. However, the technical, legal and regulatory frameworks must be in place to ensure that interoperability of data and access to information can take place. Chile has already made important progress in this area and the 2017 legislation of data protection creates the right conditions. It remains an ongoing challenge for Chile to strengthen and clarify the interoperable and standards based approach and an immediate priority should be to simplify and streamline the process by which data exchange can be agreed between two public agencies.

As Chile and its regional partners across Latin America and the Caribbean work together through networks like the e-Government Network of Latin America and Caribbean (*Red*

*de Gobierno Electrónico de América Latina y El Caribe*, Red GEALC) and the Asia-Pacific Economic Cooperation (APEC) they are beginning to consider the benefits of developing an interoperable identity framework such as the European Union's eIDAS. Such an initiative would take some time to implement but it is positive to acknowledge Chile's hosting of a Red GEALC workshop in June 2019 on #FirmaDigitalRegional looking at strengthening cross-border services and simplifying the access to services by Chilean residents in foreign countries. It is encouraging that the architectural approach being adopted to ClaveÚnica is based on international identity standards and can provide the basis for such a conversation.

### ***Funding and Enforcement***

Although there are challenges in the provision of identity being the joint responsibility of DGD and SRCel it is encouraging to see the commitment to ClaveÚnica in the funds that have been committed to support DI. Nevertheless, the absence of a single figurehead for leading the transformation of identity, and with the responsibility for its funding, means there are risks associated with coordination and delivery. This makes it critical for there to be a long-term and stable commitment for funding the transformation of identity in Chile ensuring that both physical and digital mechanisms maximise the benefits to the State and realise the potential of digital government. This would reflect the experience of the majority of countries who have established mechanisms to provide ongoing, centralised funding for a core part of the digitally enabled state so that the user experience and the functionality of the solution itself continue to evolve in response to the needs of society and the opportunities of technology

This funding needs to recognise the importance of developing a technically excellent platform with clear technical documentation to simplify integration with ClaveÚnica but also in investing in the roles of engagement and account management for 'customers' elsewhere in government that will help to communicate the value proposition and support adoption efforts.

The standardised model for business cases provides an important opportunity before any funding is committed to allow for a specific discussion around the use of ClaveÚnica. Whilst funding could be made to be contingent on the use of ClaveÚnica this may not be appropriate in all cases; should there be a situation where ClaveÚnica does not meet the needs of a given project there should be mechanisms in place for those unmet needs to be factored into the future development of ClaveÚnica. After funding has been committed Chile should use guidance and standards to consider the role of identity and the design of services which rely on it.

### ***Government services***

An effective DI is a catalyst for transforming service design. Instead of citizens needing to bring pieces of paper into offices to access services it becomes possible to prove who they are remotely, unlocking quicker and more efficient services. In Chile, only 40% of procedures can be carried out online, often because there is not a sufficiently robust identity model. Whilst the immediate priority should be to explore where ClaveÚnica can be most effectively deployed this should not come at the expense of considering how services can be transformed, especially through the *ChileAtiende* network. Indeed, a multi-channel approach to services allows for the country to consider the holistic, end to end experience of the entire service for its citizens and understand the opportunities offered by *ClaveÚnica*, even if services are not yet always accessed online. This means that the transformative

potential of DI must form part of any service standards that are developed in Chile and the quality assurance processes that accompany them.

Chile faces the challenge of reconciling the existing provision of identity with the transition to *ClaveÚnica*. Half of the transactions in Chile which are carried out online use their own authentication mechanism that is not *ClaveÚnica* and this includes the services provided by the SII. Tax offices can be an attractive partner to work with early on but this introduces challenges around migration and governance due to the critical importance of tax receipts to a country. Whether *ClaveÚnica* is the preferred solution or not, Chile should ensure that their identity strategy understands the needs of businesses and the areas of health and municipal government too.

The planned functionality of *ClaveÚnica* is to include not only data authentication but a data wallet, electronic signature, citizen mailbox and a website for managing the granting, and revoking, of permissions. The development of this approach will meet several common needs for teams across government and can reflect *Government as a Platform* thinking to accelerate the transformation of other services that would otherwise have to develop their own solutions.

### *Private sector services*

Chileans are already familiar with using the *Cédula de Identidad* to underpin their identity in interactions with the private sector. This familiarity of citizens and businesses provides Chile, and *ClaveÚnica* with an important starting point from which to consider its wider application. Moreover, that physical identity infrastructure provides the basis for a DI solution in *ClaveÚnica* that has been built with technology that is highly interoperable and easily deployed. Chile should identify the benefits to citizens, government and businesses and develop an understanding of how needs can be met across sectors. In order to do this Chile will need to establish a legal and practical framework for collaboration and partnership.

As an active member of the OECD Working Party of Senior Digital Government Officials (E-Leaders) Thematic Group on Digital Identity, Chile can draw on the extensive experiences of their peers, including **Estonia, New Zealand and Portugal**, in realising the benefits of developing *ClaveÚnica* to provide citizens with access to private sector services such as banking and telecoms.

### *Enablers and constraints*

The benchmarking study identified six areas – business model, hardware infrastructure, awareness, enrolment, user experience and societal digital literacy – that have the potential to be seen as an enabler or a constraint for DI in Chile.

The **business model** for DI in Chile should be built on the SRCeI provided identity that every citizen over 18 must have in the *Cédula de Identidad*. At this point in the development of identity in Chile, there are multiple possible models that can be explored. In doing so there should be a focus on working with both public and private sector providers to encourage adoption and deliver value.

Although the *Cédula de Identidad* does require certain **hardware infrastructure** to use its most secure features, this is not relevant for *ClaveÚnica*. Chile should instead focus on designing a DI model and user experience that takes advantage of high levels of mobile phone penetration in the Country.

Chile could invest in marketing to raise **awareness** of ClaveÚnica, but this may not be necessary given that implementation of ClaveÚnica to access services has previously been successful in driving adoption. Instead, the focus should be on designing an excellent **enrolment** and ongoing **user experience** for ClaveÚnica that makes it easy for people to adopt and embrace DI. This will rely not only on the experience of using the DI but in the quality of the services which people are accessing too.

Arguably the greatest societal value in developing and enhancing the provision of DI in Chile could be through associated **digital literacy and access** benefits. With ClaveÚnica requiring face to face interactions to initially activate the DI it is possible to combine that with skills training through *ChileAtiende* and help people to carry out their subsequent government interactions away from face to face offices and through digital services instead.

Proposals for action	Level of Priority
In light of the preceding assessments, which draw on the analysis of the 'Policy levers and adoption', the Chilean government could consider implementing the following recommendations:	
Chile should explore how to manage identity without the distinction between physical and digital in order to bring the user experience of enrolling, managing and using the two are closer together.	High
Chile should consider whether the legal requirement to be in possession of a <i>Cédula de Identidad</i> should be extended to a ClaveÚnica credentials	Low
A legal and regulatory framework must be created to manage the use of ClaveÚnica credentials to access private sector services, particularly where that opens the possibility of personal data to be reused	High
DGD should urgently review the mechanisms by which two public agencies come to an agreement to exchange data and provide guidance and boilerplate templates that support a more rapid turnaround. This should complement efforts to implement interoperability standards across both legacy and newly developed systems.	High
Explore with regional partners how to achieve interoperability of identity in a way that facilitates cross-border services and meets the needs of Chilean residents abroad	Low
Any projects or services being developed by the Chilean public sector that have a DI component should be assessed at the business case stage to ensure that they take ClaveÚnica into account. Where it is decided ClaveÚnica is unsuitable the ClaveÚnica roadmap should be updated to reflect those unmet needs and a migration plan identified for the eventual transition to ClaveÚnica	High
Funding should be made available to SRCel and DGD to develop ClaveÚnica as a reliable and respected service within government. This investment should provide for account management, simple onboarding and support with identifying return on investment	High
As Chile develops service design guidance and standards, the cross-sectoral needs (health, local government, etc.) for identity should be understood and the application of ClaveÚnica developed and enforced through the design of services which rely on it.	Medium
The development of ClaveÚnica should be considered in line with Government as a Platform thinking to accelerate the transformation of other services that would otherwise have to develop their own solutions	Medium
Chile should draw on the experiences of other members of the OECD Working Party of Senior Digital Government Officials (E-Leaders) Thematic Group on Digital Identity to develop a world leading approach to DI and private sector collaboration	Low
Use the expansion of ClaveÚnica as an opportunity to provide digital literacy and digital skills training to citizens through <i>ChileAtiende</i> and other face to face locations whilst people are activating their ClaveÚnica for the first time	Medium

## Transparency and monitoring

### *Citizen control of their data*

The future ambition for ClaveÚnica in terms of how much control it will give to citizens is at the cutting edge of how governments are thinking about the relationship between citizens and their data. Placing the citizen in control of their data through the provision of a data wallet and developing an online experience where they can control who has access to what, could become a model for other countries to emulate. This will require that the vision, leadership and funding are provided to enable ClaveÚnica to deliver on that promise as well as a commitment to interoperability between government services and the participation of a suitably informed, appropriately trained and sufficiently trusting public.

### *Performance data*

In measuring the performance of DI there is a risk of adopting overly simplistic measures to gauge adoption like the number of active accounts. This might help to show penetration of DI in the population but its value is best understood in the context of the services it transforms. Therefore, it should be a priority for Chile to identify Key Performance Indicators (KPIs) that can be measured by identity reliant services, regardless of whether or not they are currently using *ClaveÚnica*. Such KPIs could consider the length of time it takes to process an application without DI, the costs incurred due to errors introduced by an analogue identity process that subsequently need to be resolved, or the quantifiable damages caused by criminality. These will help demonstrate the relative benefits of migrating to *ClaveÚnica* compared to the status quo. Once the KPIs are identified they should be incorporated into the impressive open performance dashboards for *ChileAtiende*.

A less public but equally important consideration of measuring performance should be on the internal expectations placed on senior officials across the public administration. By establishing *ClaveÚnica* as the strategically agreed model for DI for government services in Chile performance indicators that link individual leadership achievements to its implementation could help to reduce the duplication of effort on alternative models of DI and ensure a more collective and coherent approach to DI.

### *Impact assessment*

One of the most important pieces of information for a country evaluating the impact of its DI approach is a clear cost-benefit analysis of both the solution, in Chile's case *ClaveÚnica*, and the experience of individual adopting services. However, the study has shown that in general this is not always a priority. Providing a political mandate is important, but accountability and analysis is still required to ensure that the approach to DI is, and continues to be, the best fit for the issues being addressed.

As Chile implements DI they should be clear about the costs, and the benefits, of their chosen model and use the analysis of return on investment to prioritise features and to target adopting services. In considering costs it is important for Chile to be realistic about the different nature of costs that will be involved during the development, implementation and operating stages for different models of DI. Should Chile continue to use the SRCeI as the basis for *ClaveÚnica* then initial development costs will be minimised, but there are different costs associated with the ongoing operation of the face to face network provided by the SRCeI and the physical identity card.

This exercise is not only important for proving the value of *ClaveÚnica* to political leaders, who are committing funds to its development, but will help government teams, and private sector companies, make the case for developing solutions and services that use *ClaveÚnica* and simplify arguments about adoption. Doing this analysis against agreed baselines will also help to clearly, and quickly, demonstrate whether any of the assumptions in the business case need to be revisited and the projected costs and benefits revised accordingly.

Proposals for action In light of the preceding assessments, which draw on the analysis of 'Transparency and monitoring', the Chilean government could consider implementing the following recommendations:	Level of Priority
In line with Chile's ambition to put citizens in control of their data, which is to be commended, Chile should commit the funding and resources to continue exploring the feasibility of this approach and, should the value be proven, develop it as the approach to DI	<b>High</b>
Key Performance Indicators that identify the time and cost involved in providing services without DI should be implemented to offer a baseline for comparing and demonstrating the benefit of implementing DI. Publish this as Open Government Data and within the performance dashboards detailing the quality of service provision in Chile	<b>High</b>
Make senior public officials whose roles have a bearing on the use of DI solutions accountable for the adoption of ClaveÚnica by including relevant targets for government-wide implementation within their personal performance assessment.	<b>Low</b>
Chile should produce a clear cost:benefit analysis and rationale for identifying return on investment to support service teams in adopting ClaveÚnica and making the business case for its ongoing funding	<b>Medium</b>

## 1. Introduction

*This opening chapter introduces the challenges of digital identity (DI) and its importance in underpinning digital government approaches to the transformation of policymaking and service delivery.*

*It also introduces the scope of the analysis and the framework being applied to Chile's experience with DI in the context of the comparative experience of 13 countries who provided their insights for this research: Austria, Canada, Denmark, Estonia, India, Italy, Korea, New Zealand, Norway, Portugal, Spain, United Kingdom and Uruguay.*

In our interactions with the people we know we don't give any thought to the proof of their identity. When we meet someone for the first time we trust that they are who they say they are. Sometimes an introduction is brokered by another person, a mutual, trusted, acquaintance who knows both parties. However, in our transactional dealings with businesses and government there is a greater expectation of being able to prove who we are, where we live and what we can access.

There is therefore a need for identity to be provable, but how do we know somebody is who they claim to be? How would I demonstrate to you that I am the person I'm claiming to be, a person born in a particular place, living at a certain address and having the legal standing to do business, cross borders, access medical care and generally go about life in any of a myriad different ways.

From the other side of those questions, how does government have confidence that they know who is entering and leaving their country? How do they safeguard citizens from crime by identifying perpetrators and bringing them to justice? How do they make sure only trusted parties access and alter data related to citizens, business and organisations? How do they make sure services are accessed only by those with the entitlement?

Box 1.1. A timeline of identity verification briefly traces the evolution of identity proof from origins of the significance of how people dressed or marked their bodies through to the development of physical tokens that would be carried. The original of these was the 'passport', a document not created with identity in mind but as a form of protection for the holder in passing through foreign countries based on an association with their home nation.

Over time, records of birth, marriage and death have been adopted to confirm verifiable sources of fact about an individual's life whilst licences for driving, practicing a particular profession or operating a business form part of the legal framework for regulation of the state. These documents underpin many of the most significant face to face interactions which take place and act as the mechanisms by which activities are policed, in person.

In many countries, these needs have given rise to the creation of a multi-purposed identity document. The ubiquitous 'ID' allows people to prove their age for leisure pursuits, register at hotels when travelling, or confirm to authorities that the person they have in front of them is the person they think they're looking at. Such devices have been open to abuse and introduce vectors for counterfeit and fraud resulting in ongoing evolution in the technology underpinning these tokens. Nevertheless, the challenge of face to face identity validation is supported by a mature and accepted model.



### Box 1.1. A timeline of identity verification

100 000 years ago	Displaying jewellery or other decorative goods
2000BC	Tattoos and skin markings
209BC	The first written census in Rome
1414	English King Henry V invents the first passport
1829	UK Prime Minister Robert Peel links personally identifiable information to a unique number
1870	Sir William Herschel pioneers the use of fingerprinting for precise identification
1936	US introduction of a physical social security number card
1980s	The first government smart cards are issued in Germany, Spain, Czech Republic, and Singapore
1986	First use of DNA in criminal proceedings
2005	The OpenID protocol is created to support LiveJournal (ultimately being supplanted by OAuth)
2009	Launch of Aadhaar, the world's first government backed biometric identity platform

Face to face processes were built on top of these existing identity mechanisms. As that model has matured it has come to underpin the delivery of public services. With countries turning their attention to facilitating access to government services online, the e-government agenda has created a new challenge – the need of being confident in the identity of someone who is not physically present.

With an increasing desire to see public services **on the internet** this has been a priority for many countries with investment in technology to accompany it. Generally the incremental approach of this shift has meant that countries took existing processes, and existing interactions, and digitised them as they were with the result that in those cases where a ‘wet signature’ was still required it produced services that were mostly online, but which would ultimately require offline steps to complete.

Technology has been applied to this problem through creating digital signatures and the increasing adoption of password based account services introduced new modes of service delivery but more often than not these were ad hoc solutions, poorly coordinated and resulting in multiple variants on authentication credentials for government, and citizens, to contend with.

As more and more countries explore how to shift their services online in a way that is digital by design and recognises the importance of providing services that meet the needs of their

users these existing interactions have been shown wanting in satisfying the burden of proof required by more advanced public services.

Thus, as countries explore how to implement public services **of the internet** they have turned to new models of digital identity (DI) to enable the transformation of the experience of the state. Those countries who have attempted to respond to these issues have found themselves subject to the increased expectations of a public who are used to simple, interchangeable identity mechanisms provided by existing accounts created with Google and Facebook. However, such approaches to identity lack the substance required to confidently confirm that the absent party is who they claim to be.

Whilst countries wish to benefit from the digital transformation of their services they must remain mindful of threats from hostile forces, fraudulent behaviour and the errors of their users. The resulting challenge for government is therefore to respond to the needs of their citizens, businesses, and visitors, whilst also balancing the concerns of a public which views government over-reach as a dangerous thing.

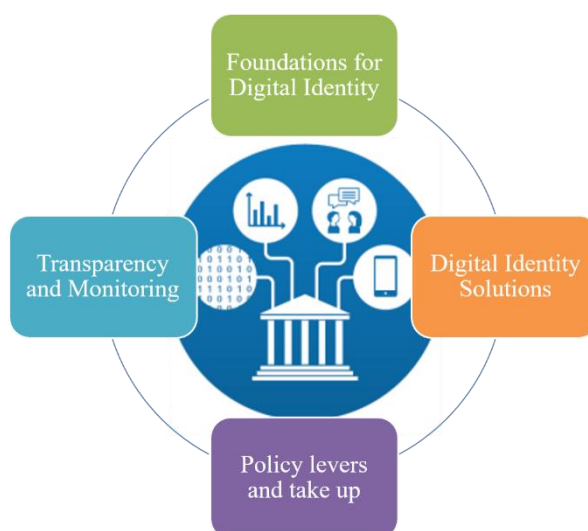
DI is required for people to exploit the digital economy and interact with a digital government. It provides the link between authentication and claims about a person's identity which are a fundamental enabler to transformation in government and business.

DI enables omnichannel services, giving users choice over the most effective service channel whether through a browser, on a mobile device or over the telephone. At the same time, DI supports moving away from analogue experiences of proving identity, and enables the redesign of user experiences to create more efficient organisations and more ambitious services. This is particularly relevant in the case of government where DI enables interoperability, empowers the exchange of electronic data, and can transform processes and services that are better focused on meeting people's needs.

To gather best practices and compare the developed solutions from different cultural, social and economic contexts, 13 approaches for DI were assessed to elaborate the analysis include in this Study<sup>1</sup>, namely in **Austria, Canada, Denmark, Estonia, India, Italy, Korea, New Zealand, Norway, Portugal, Spain, United Kingdom and Uruguay**. Following the initial evidence provided by these countries, the OECD followed up with a selection of these (**Austria, Canada, Italy, Spain, Portugal and the United Kingdom**) to further develop some of the themes.

The impact of DI on the digital transformation of the public sector is assessed with the scope detailed in Figure 1.1. It considers the context for delivering DI in terms of the initial foundations, DI technical solutions, the level of take-up, and the post-implementation monitoring mechanisms in place.

**Figure 1.1. DI assessment scope**



## DI assessment framework

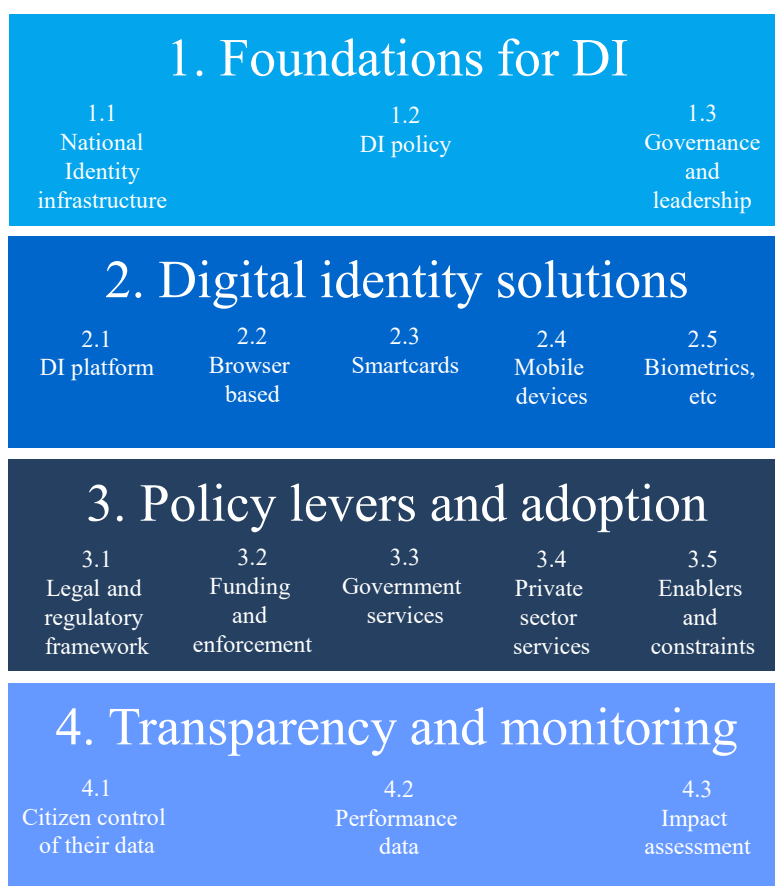
Following this scope, Figure 1.2 indicates the expanded dimensions being considered. First, in presenting the Foundations for DI there is an analysis of national identity infrastructures, the content and focus of DI policy, and models of governance and leadership.

Secondly, the DI solutions built on those foundations to deliver DI policy are considered. This analysis explores the features, requirements, and channels (for use and enrolment) across single factor, smart card, mobile, and biometric systems.

Thirdly, the rate of adoption for DI solutions is helpful in understanding the effectiveness of a given model and its supporting governance. The role of policy levers in areas of legal and regulatory frameworks and models for funding and enforcement are considered alongside the impact and adoption of DI on the digital transformation of government, the private sector, and society through exploring the services that result given the context in which they operate

Finally, these approaches are examined in the context of their transparency about access to an individual's data, their openness about performance data and the ways in which impact is assessed.

Figure 1.2. DI assessment framework



## Note

<sup>1</sup> The information presented in this report from India and New Zealand was gathered through desk research. The information presented in this report from Austria, Canada, Denmark, Estonia, Italy, Korea, Norway, Portugal, Spain, United Kingdom, and Uruguay was gathered through desk research and OECD survey answers.

## 2. DI in selected countries

*This chapter presents a comparative analysis of the DI experience in 13 countries through each dimension of the analytical framework explained in Chapter 1 based on a survey completed by the countries.*

*The assessment compares the foundations for identity in terms of existing national identity infrastructure, policies supporting DI and a country's governance mechanisms.*

*DI solutions are then analysed with a discussion of the technical approaches for browser, smartcard, mobile, and biometric based systems.*

*The policy levers and adoption of DI are assessed in light of the legal and regulatory framework, funding and enforcement measures, the services made available, and the enablers and constraints identified by the countries.*

*The ways in which citizens are being put in control of their data, the openness with which countries are sharing the results, and their approaches to impact assessment are described in the last dimension.*

*Finally, trends identified in the study are presented.*

## Dimension 1: Foundations for DI

The foundations for DI are the tools, policies and governance structures, which support the development and implementation of DI in a country. This section begins by considering the different approaches to identity infrastructure within a country that underpin DI registration and access. Following this the approach to policy in the areas of security, interoperability, user experience and privacy is discussed. In conclusion the different approaches to governance are described, with a particular focus on the interactions between private sector and government.

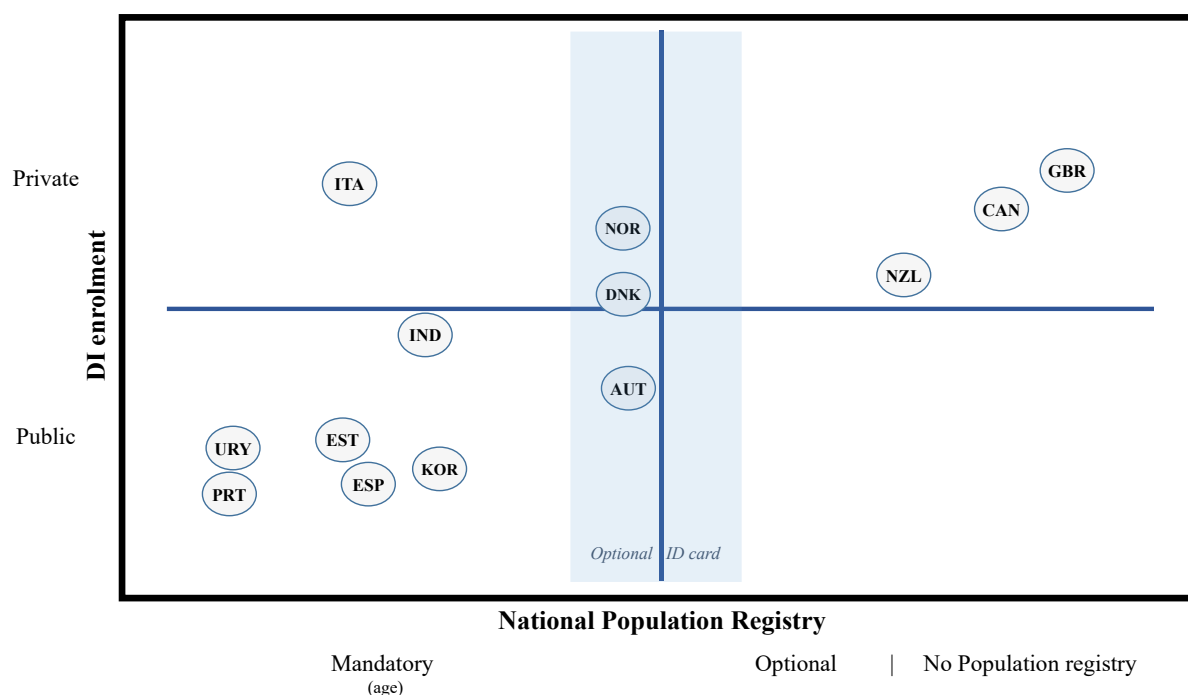
### *Dimension 1.1: National identity infrastructure*

National population registers are used as the source of information for the initial registration of digital identities in several countries. However, due to social and cultural reasons other countries do not have such national identifiers or, if they do, prefer not to attach DI to them. The following approaches for the role of national ID in DI have been observed:

- DI is **supported by a public, centralised register of the population**. Linking DI to a national population register was found in **Austria, Estonia, India, Korea, Portugal, Spain, and Uruguay**, and tends to increase usability and utility.
- DI is **supported by a public, decentralised register of the population**. In some countries there is no single national population registry but several population registers which are linked to a citizen's DI. Since 2014, **Italy** has a centralized National Resident Population Register (ANPR); municipalities are still migrating into ANPR; yet, forecasts indicate that by the end of 2019, the number of citizens in ANPR will be more than 45 million over a population of 60.55 million
- DI is **verified or provided by several private and public organisations**. This approach is being taken by those countries which do not have a national population registration system providing a unique number for all the population as in **Canada, New Zealand** and the **United Kingdom**; or where DI efforts have historically been led by the private sector as in **Denmark** and **Norway**.

Figure 2.1 shows how countries which rely on national population registers, require mandatory registration for the whole population. This is either from the first days of life (for example in **Portugal** and **Uruguay**), or before adulthood (in **India** and **Spain**). In **Portugal** the “*Born Citizen Project*” (*Nascer Cidadão*) enrolls citizens on the population register and provides a national ID card (*Citizen Card*) in the medical facility when a child is born.

Figure 2.1. Digital ID enrolment and National Population Registers



Source: Based on information provided by Austria, Canada, Denmark, Estonia, India, Italy, Korea, New Zealand, Norway, Portugal, Spain, United Kingdom and Uruguay in response to the OECD survey Benchmarking Digital Identity Solutions (Unpublished)

There is a strong correlation between a country not mandating registration in a population register or not having one, and private sector responsibility for DI enrolment. This is seen in **Canada**, **New Zealand** and the **United Kingdom** where the absence of mandatory public population registers means greater involvement for private entities in managing DI. Where both registration in the population register and national ID cards are mandatory, private sector involvement is lower (**Estonia**, **India**, **Korea**, **Portugal**, **Spain** and **Uruguay**) with the exception of **Italy** where, at least within the SPID identification scheme, the private sector plays a part. Finally, for those countries with national population registers but optional national ID cards there are differing levels of involvement for the private sector, with more in **Denmark** and **Norway**, and less in **Austria**.

#### *Characteristics of National ID cards*

Six of the countries in this study (**Estonia**, **India**, **Korea**, **Portugal**, **Spain**, and **Uruguay**) have both a national population register and a mandatory national ID Card. **Austria**, **Denmark**, and **Norway** also have national population registers but an optional or sectorial ID card. . Finally, the three countries without a national population register, **Canada**, **New Zealand** and the **United Kingdom**, do not have national ID cards; in this case, government services are usually accessed through verification by private entities (namely banks, and postal services). In **Italy**, the issuance of the ID card is mandatory; and since 2019 is mandatory to issue the Electronic ID (CIE) and as a result municipalities no longer issue ID cards in paper format.

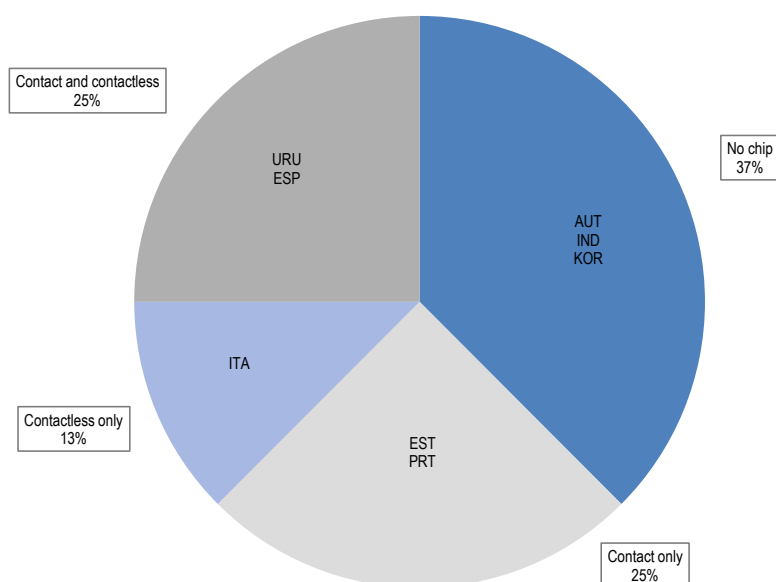
The countries which issue ID cards do so using polycarbonate and according to the standard format ISO/IEC 7810:2003 ID-1 and feature the following elements:

- **Identification of the country**
- **Citizen photo**
- **Biographic information including the name, birthdate, nationality, and biological sex of the holder**
- **Validity information such as the date of issue, or of expiry and the document number**
- **A reproduction of the card holder’s signature**
- **A representation of the data contained on the card encoded in a machine readable format, known as the Machine Readable Zone or MRZ**
- **Physical card security features including holograms and holographic symbols, embossing, variable colour printing, fluorescent elements, and elements visible only under ultraviolet light.**

Whilst the materials of the cards are alike, there are differences in how chips have been incorporated as shown in Figure 2.2. Five countries feature electronic chips whilst **Austria**, **India** and **Korea** do not. **Estonia** and **Portugal** have chips that require contact to be read, **Italy** has a contactless chip and **Spain** and **Uruguay** have a dual interface allowing for both contact, and contactless, reading of the card.

It is noteworthy that ID card systems which have recently been developed or upgraded, as in **Italy**, **Spain** and **Uruguay**, favour contactless. The adoption of this technology reflects the increasing use of ID cards for access control purposes (for example in transportation and at border controls) and the prevalence of mobile devices with near-field communication (NFC) capabilities for public servants to access data on cards ‘in the field’ (for example in relation to enforcement activity).

**Figure 2.2. Chip technology incorporated into national ID cards**



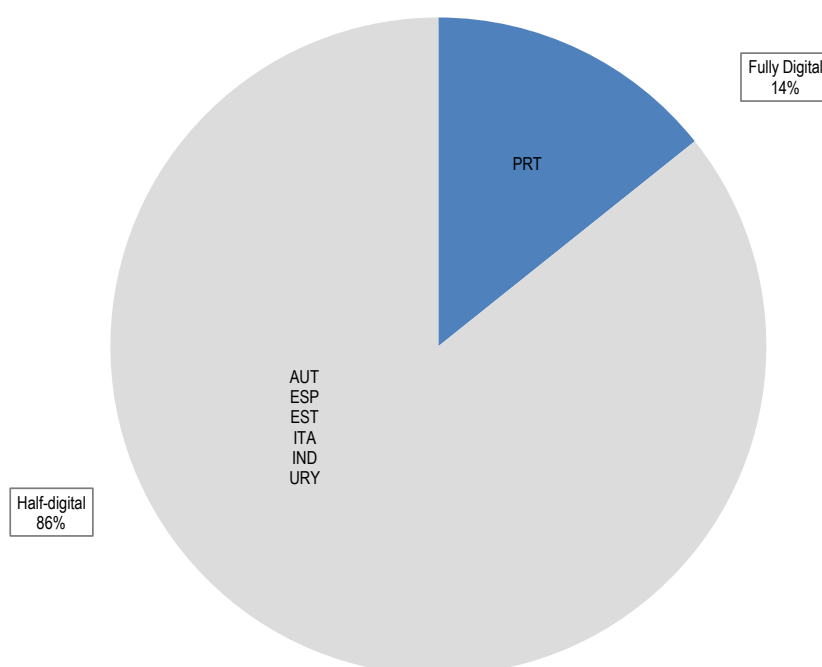
*Source:* Based on information provided by Austria, Estonia, India, Italy, Korea, Portugal, Spain, and Uruguay in response to the OECD survey Benchmarking Digital Identity Solutions (Unpublished)



Face to face interactions are increasingly expensive for both users to access and the government to provide. Therefore, moving enrolment for national ID cards away from such processes is attractive. However, due to the nature of identity this presents security challenges. Remote processes that incorrectly identify a person, or which are subject to fraudulent subversion, undermine the authenticity of an identity and therefore any subsequent DI approach which reuses these flawed, or corrupted, data.

All countries with national ID cards handle the application process online at least in part. Figure 2.3 shows that only in **Portugal** is the enrolment process fully digital with the remaining countries using paper based forms or the submission of physical photographs or certificates. Alongside this all countries provide an in person enrolment process with **Estonia** additionally allowing the request of an ID card by post.

**Figure 2.3. Approach to enrolling for an ID card**



*Source:* Based on information provided by Austria, Estonia, India, Italy, Korea, Portugal, Spain, and Uruguay in response to the OECD survey Benchmarking Digital Identity Solutions (Unpublished)

In **Portugal**, the national ID card (*Citizen Card*) can be renewed online in certain conditions. To do this it reuses previously provided biometric data (from existing photographs and fingerprints) and requires in-person collection from a *Citizen Shop*. When claiming the card the recipient must perform a fingerprint match to verify their identity. This two factors approach allows for a reduction in the costs of application whilst maintaining the integrity of assurance for the ID card.

Whilst the costs may reduce for the government, the addition of extra technology to the cards themselves does increase the cost for citizens. There is a wide variance in terms of how much it costs a citizen to obtain their national ID card with **Uruguay** citizens needing to pay EUR 7.40 compared to **Austria's** EUR 61.50.

### *Dimension 1.2: DI policy*

The policy approaches required by countries to implement DI share several common features. In most countries, the following priorities are clearly visible:

1. Improve user experience
2. Provide digital access to government services
3. Increase security
4. Transform the digital economy (including private sector services)
5. Reduce the cost of doing business in the country

DI is a clear enabler for transforming the user experience of services. Many of the countries considered by this study are focusing on how they might apply the concept of **digital by design** to the experiences of citizens, reducing the requirement for paper processes and offline interactions in meeting a need by being confident in the identity of the person accessing the digital service. Thus, the approach taken to DI is often influenced by how a country has recognised these challenges in their National Digital Strategies, assurance processes, capability building and design guidelines.

More than half of the countries in this study were explicit that their commitment to DI was a policy decision designed to establish a common authentication approach across government services. The concept of a single sign on for government is attractive in simplifying interactions between citizens and their services but relies on the interoperability of data between different parts of the government. One response to this, demonstrated particularly well by **Estonia** and **Portugal**, is found in accessing professional attributes from third parties with responsibility for managing the data. In order to make such **attribute exchange** possible, DI policy needs to ensure the interoperability and reuse of data between public and private sources.

The starting point for DI policy is ensuring that there is confidence that the person using a DI is the person it belongs to. This requires confidence in the way in which an identity is generated in the first place but also that the model of DI is capable of responding to criminal threats and user error. Given the sensitivity of the information countries were unable to share extensive details for publication about how they respond to the security threats identified by their DI models. Nevertheless, provision is made within national digital security strategies to ensure that approaches to DI are **secure for government, and for users**. In the **United Kingdom** the nature of how GOV.UK Verify is built and maintained means considerations of security at scale are part of the solution's design and the product team that exists to support it.

Whilst it is important for government to have confidence in the security and usability of its DI model, it is arguably most important that it has **the trust of its users**. In this respect, DI policy reflects wider governmental trends concerning data protection, the transparency of access to personally identifiable information, and the mechanisms by which citizens might grant consent for its access or reuse. Several DI approaches include opportunities for user to actively grant consent for their data to be used with the experience of **Austria** discussed in more detail in Box 2.1.

### Box 2.1. Austria SourcePIN and ssPIN

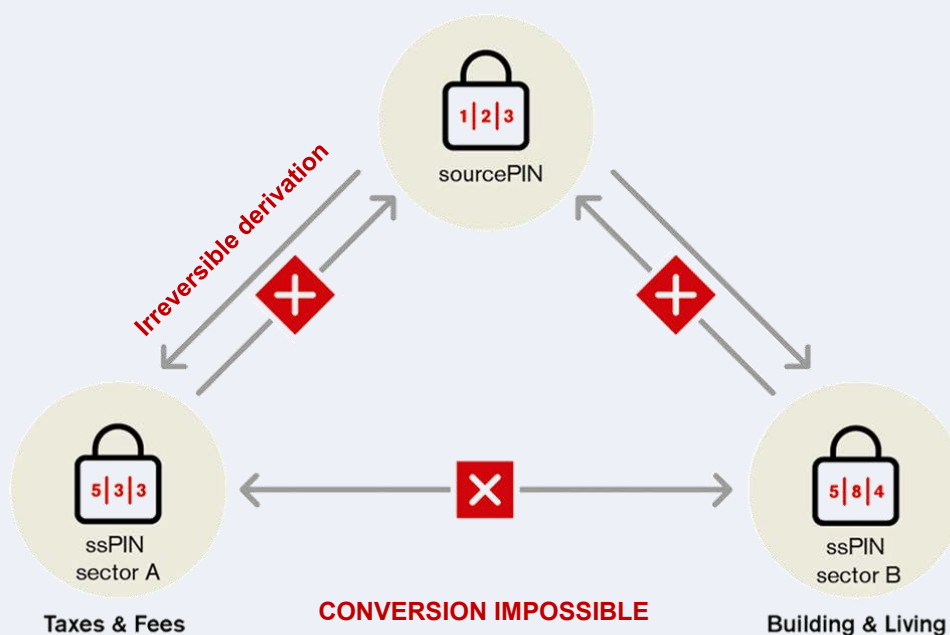
In **Austria** a SourcePIN is required for the unique identification of a citizen. This number is generated from the SourcePIN Register when required and deleted afterwards. Citizens are able to access an audit trail detailing how their data have been accessed and used.

In general, this will not have happened without the user knowing as public authorities are not allowed to save the SourcePIN of a citizen. Instead, they use a sector-specific personal identifier (ssPIN), which can only be used for a particular purpose during a particular timeframe. The ssPIN is derived from an individual's SourcePIN through a non-traceable and irreversible cryptographic process.

To generate an ssPIN, a public body must have the explicit agreement of the person concerned with this consent only providing validity to the ssPIN for use according to the activity under which the initiated procedure falls. It cannot be used to access services in another sector.

Only the SourcePIN Register Authority may generate an ssPIN without the citizen card of the person concerned, and it may do so only in special circumstances with the help of adequate identification attributes.

**Figure 2.4. Austria SourcePIN and sector-specific personal identifier**



Source: Digital Austria (Austrian Government Federal Chancellery, 2017<sup>[1]</sup>)

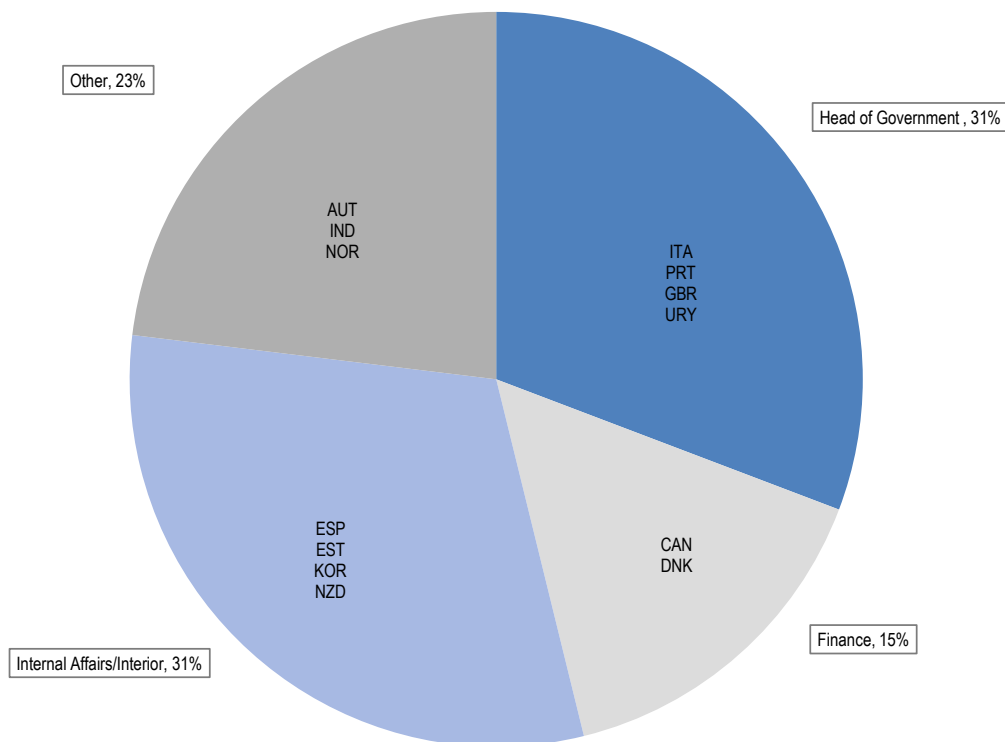
### Dimension 1.3: Governance

Governance covers the leadership and development of politics, policies and processes surrounding the implementation of DI and in particular brokering relationships between public and private actors involved with DI.

The models for DI governance are often aligned with how countries are promoting their Information Technology and digital government agendas. There is a strong correlation between those organisations which are responsible for digitally transforming the experience of public services, and those which hold political or operational responsibility for DI governance. This decision reflects the importance of DI in enabling the ambitious redesign of services and the transformation of government.

Figure 2.5 shows the four categories of political leadership identified across the 13 countries in this study. In four of them (**Italy, Portugal, United Kingdom and Uruguay**), responsibility is closely associated with the head of the government (Prime Minister office, or with the President of a Council of Ministers). The same number of countries (**Estonia, Korea, New Zealand and Spain**) locate this responsibility within the Internal Affairs or Interior Ministry. **Canada and Denmark** look to the Finance Ministry whilst the other three countries (**Austria, India and Norway**) house the responsibility in specific ministries focused on digitalisation.

Figure 2.5. Political leadership of DI



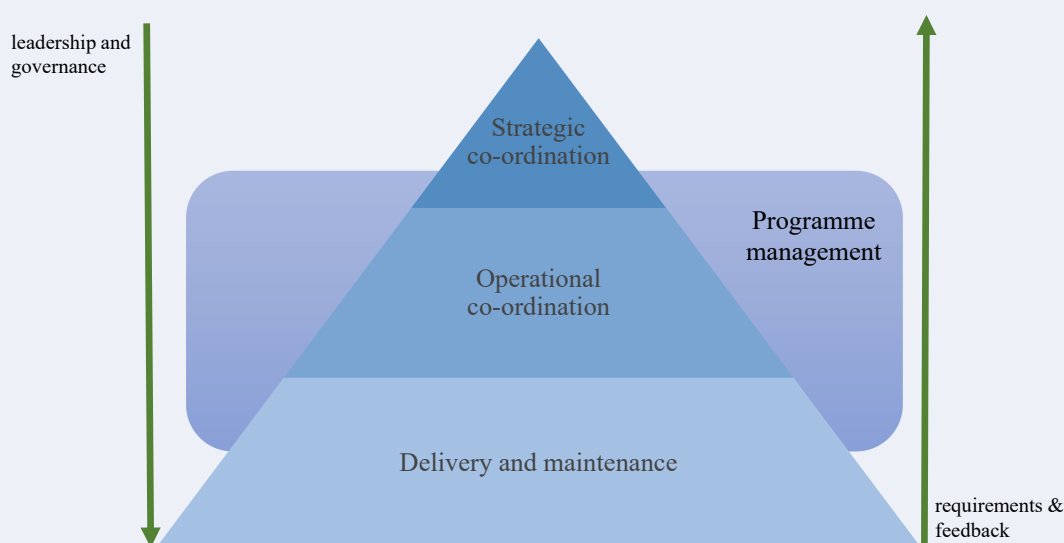
Source: Based on information provided by Austria, Canada, Denmark, Estonia, India, Italy, Korea, New Zealand, Norway, Portugal, Spain, United Kingdom and Uruguay in response to the OECD survey Benchmarking Digital Identity Solutions (Unpublished).

### Box 2.2. Portuguese DI governance

The Portuguese Governance Model aims to ensure both the implementation and monitoring of the DI programme, and the strategic and operational coordination of the National DI ecosystem.

The governance model is organised across three levels, supported by a Programme Management layer.

Figure 2.6. Portuguese governance model



The **strategic coordination** level establishes a common vision for DI in Portugal. The political leadership of the National DI involves the ministry responsible and the president of the council of ministers, along with other relevant ministries for DI (e.g., Internal Affairs, Finance, Justice, Social Security, and Health). Permanent bodies reporting to this leadership have direct responsibility for policy making, monitoring and assessing DI initiatives.

The **operational coordination** level pursues the policies and vision set by the national leadership. This aggregates those responsible for the functional blocks of Portugal's DI ecosystem.

The **delivery and maintenance** level implements projects and runs the ecosystem of DI components. Operating through the direct authority of those in the operational coordination level this is done through responsible the public or private entities.

Given the organisational, functional and technological diversity of the Portuguese DI ecosystem, a programme management office (PMO) is in place. The PMO participates throughout the DI program, establishing measures, planning and monitoring the execution of the guidelines outlined, and ensuring visibility of DI across the country.

*Source:* Provided by Portugal in response to the OECD survey Benchmarking Digital Identity Solutions (Unpublished)

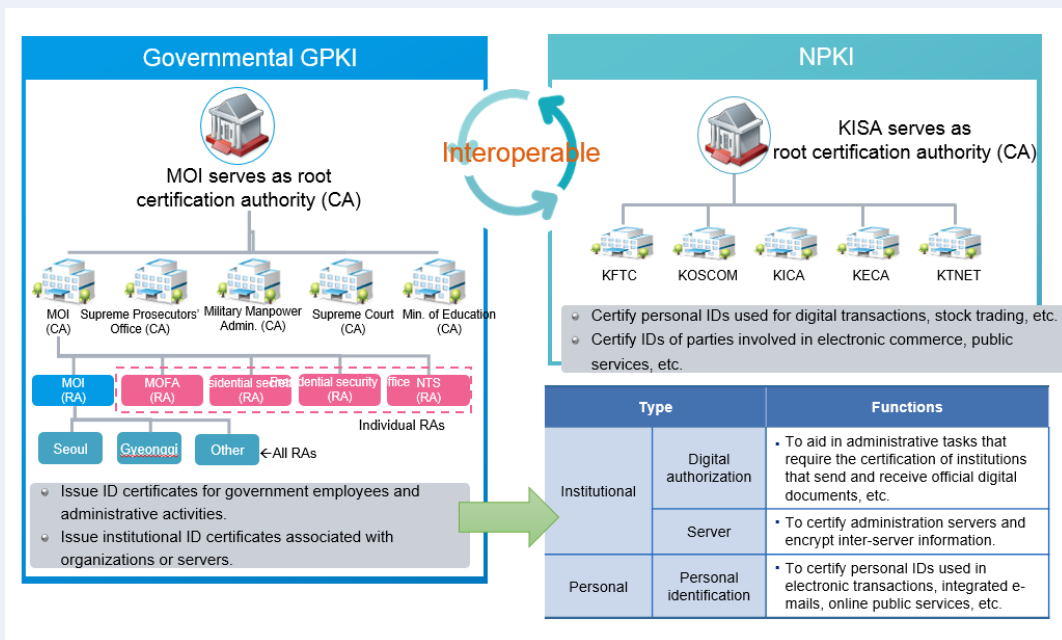
DI systems, which use digital certification for authentication and also support digital signatures on documents, are often built on top of a Public Key Infrastructure (PKI). Governance of this approach is managed through the same ministry responsible for DI, with the example of **Korea** discussed in Box 2.3. Such DI solutions are discussed in more detail in Dimension 2.3: Smartcards and Dimension 2.4: Mobile.

**Box 2.3. Public Key Infrastructure governance in Korea**

The Korean Government implemented both a National Public Key Infrastructure (NPKI) and a Governmental Public Key Infrastructure (GPKI). The use of GPKI was facilitated as the Government promoted the use of e-document among government agencies. In 2002 the use of NPKI became mandatory for online banking with the requirement for NPKI subsequently applying to all electronic transactions.

The Ministry of the Interior and Safety (MOIS) serves as the Root Certificate Authority (CA) for GPKI and the Korea Internet Security Agency (KISA) does so for NPKI. Both PKI solutions are interoperable.

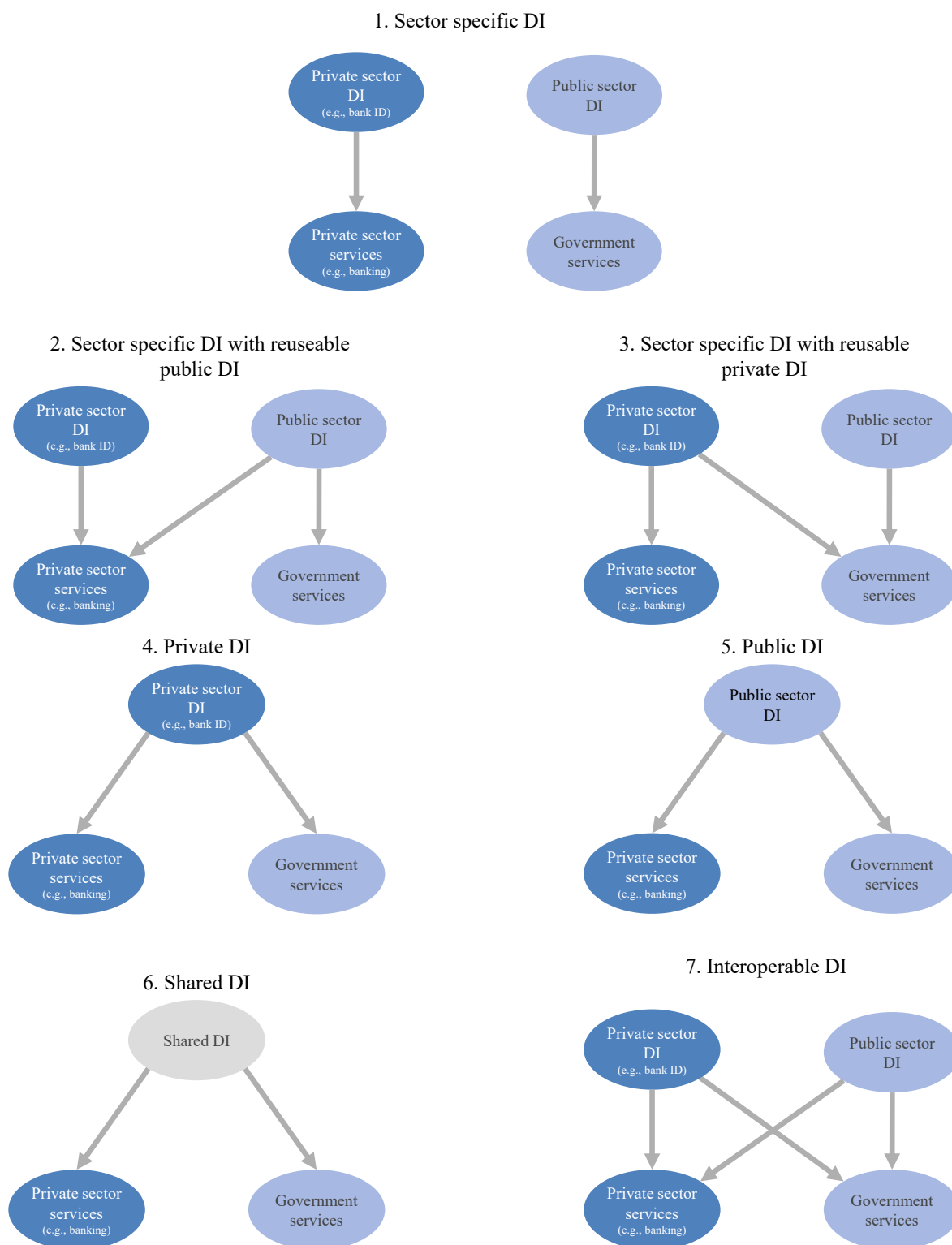
**Figure 2.7. Relationship between Government and National Public Key Infrastructures**



Source: Provided by Korea in response to the OECD survey Benchmarking Digital Identity Solutions (Unpublished).

National approaches to DI may be developed by the public sector (often from scratch) or based on the reuse of existing solutions already provided by a country’s private sector. The relationship between private and public sources and application of identity is important in shaping the effective use of any DI. Figure 2.8 explores 7 theoretical models for exploring the relationship between public and private sector solutions and their reuse in accessing services.

**Figure 2.8. Models for issuing, managing and using DI**



*Source:* Based on information provided by Austria, Canada, Denmark, Estonia, India, Italy, Korea, New Zealand, Norway, Portugal, Spain, United Kingdom and Uruguay in response to the OECD survey Benchmarking Digital Identity Solutions (Unpublished).

In Model 1 (“Sector specific DI”) private and public entities remain separate with private DI used in private sector services and public DI used for government services. This model is seen in **Uruguay**.

Model 2 (“Sector specific DI with reusable public DI”) has clear separation between private and public DI but enables the reuse of public DI to access certain private sector services. This model is seen in **New Zealand, Portugal and Spain**. The inverse approach to this, captured in Model 3 (“Sector specific DI with reusable private DI”), is not evidenced in the countries selected for comparison.

In Model 4 (“Private DI”) users can access both private sector and government services using a single, reusable DI, provided and managed by the private sector. This model is found in **Norway**.

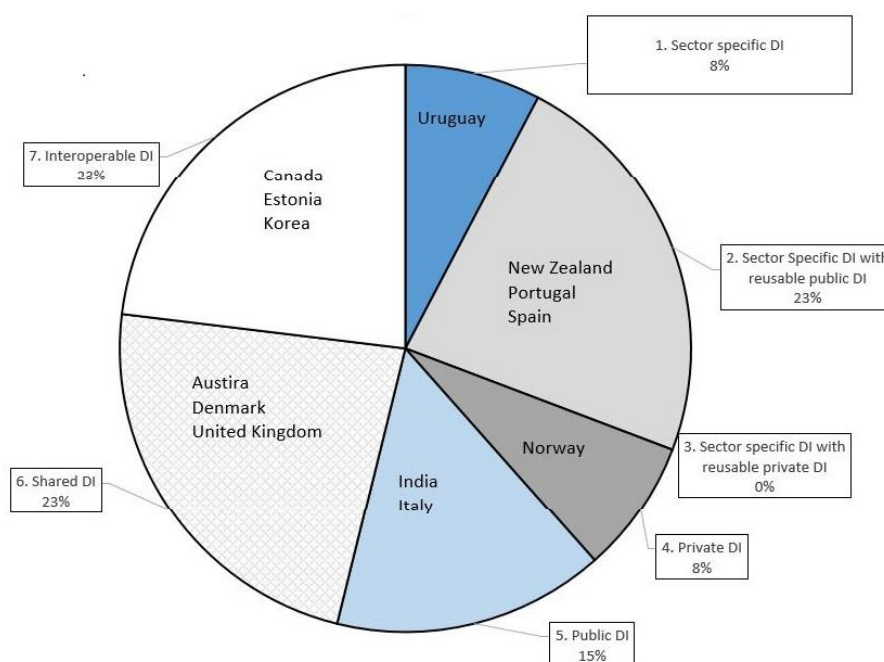
**India and Italy** demonstrate Model 5 (“Public DI”) where a single, reusable DI provided and managed by the public sector is available to access both private sector and government services.

Users in **Austria, Denmark** and the **United Kingdom** (more detail on GOV.UK Verify can be found in Box 2.4) can access both private sector and government services via Model 6 (“Shared DI”), with a single, reusable DI where responsibility for its issuance and management is shared between government and the private sector.

Model 7 (“Interoperable DI”) allows for the creation of identity by both private sector and public sector entities but with an interoperability that allows for its reuse to access services of any type. This model is found in **Canada, Estonia and Korea** where the NPki is the only digital certification for authentication for the citizens and it can be used for both government services and private sector services such as banking. The NPki is managed by KISA, an affiliate agency of the Ministry of the Interior and Safety and issued by pre-authorized financial entities. Therefore, it is regarded as public DI.



**Figure 2.9. DI models found in selected countries**



*Source:* Based on information provided by Austria, Canada, Denmark, Estonia, India, Italy, Korea, New Zealand, Norway, Portugal, Spain, United Kingdom and Uruguay in response to the OECD survey Benchmarking Digital Identity Solutions (Unpublished).

### Box 2.4. GOV.UK Verify

GOV.UK Verify is a federated identity system managed by the UK government. Direct responsibility for the programme is held by the Government Digital Service, a unit of the Cabinet Office which fulfils a central coordinating function close to the Prime Minister and their senior ministers.

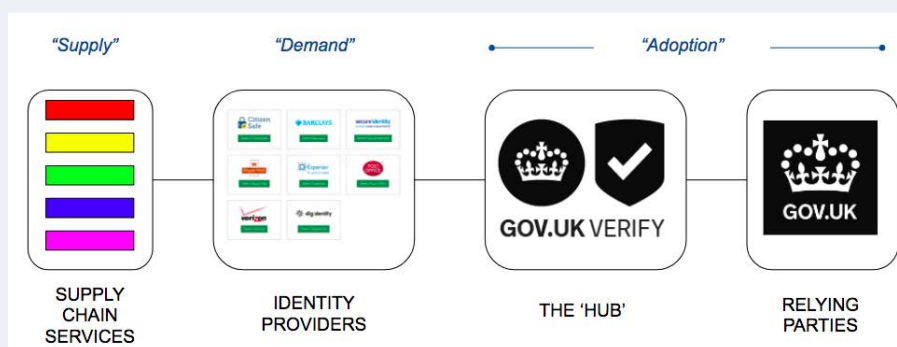
This federated approach means the identity infrastructure behind the UK's DI is not run by the government. Instead of receiving an identity from the government, a user registers with a certified company of their choosing who verifies their identity. When a user uses a service requiring a verified identity the user is passed to their chosen certified company, having authenticated with them the certified company communicates that verification to the service being accessed and the user returns to complete their transaction.

Nevertheless, the government maintains an important role in providing the user journey from GOV.UK, the UK's single government website to the different identity providers. Moreover, the Government Digital Service team provides an important role in setting standards for the onward user experience, and working with the industry to agree protocols and standards covering identity proofing, verification and authentication.

Certification for identity providers is based on those protocols and standards. The UK government publishes guidance that explains the standards a certified company has to meet, and how they can meet them, rather than specifying technologies or processes. Once certified, these companies have to demonstrate an ongoing commitment to appropriate information security arrangements and are assessed by tScheme for the quality of their service. They also have to pass a number of rigorous contractual 'gates' at which they demonstrate to government that their solutions meet any contractual requirements.

UK hub and supplier services are developed based on openly published standards and Good Practice Guides (GPG's) developed with government departments and industry partners. The government sets standards for services requiring minimal, or in-depth, evidence for citizens to prove their identity. Each UK government department decides how much evidence is required in order for citizens to access each of its digital services.

**Figure 2.10. GOV.UK Verify conceptual architecture**



Source: GOV.UK Verify (UK Government, 2018<sup>[21]</sup>)

Governance models with a focus on the public sector are easier to manage and implement due to avoiding the need for operability with external private systems. However, as the

private sector may already have DI solutions, those models which do not promote cooperation between the sectors see lower levels of DI reuse. Solutions that reuse existing (private) DI, develop a shared model, or consider public and private sector applications tend to ensure higher adoption of DI by services in both the public and private domains.

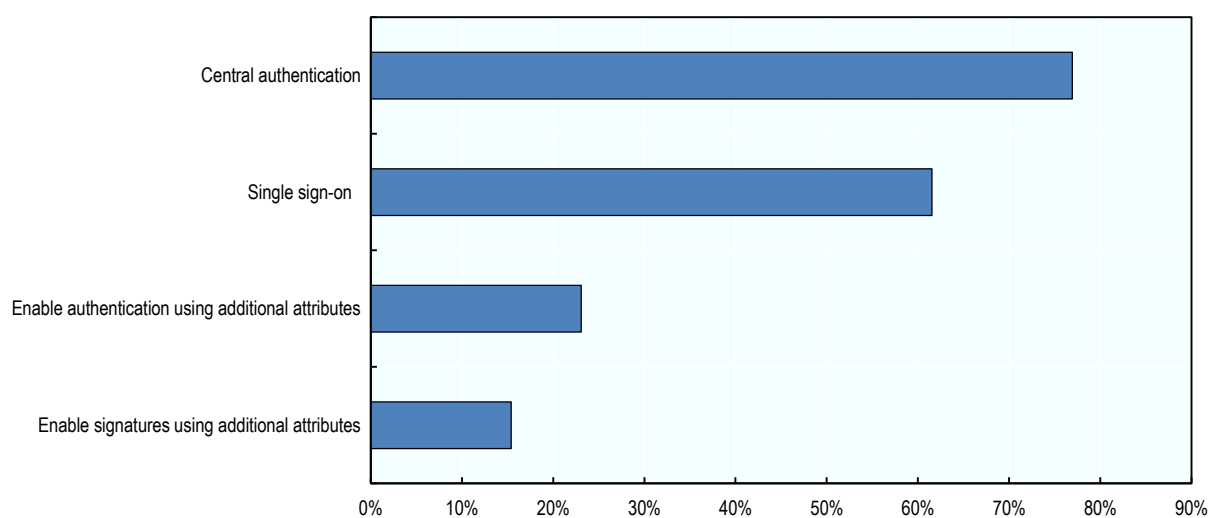
## Dimension 2: DI Solutions

This section explores DI solutions in the selected countries. The platforms are described in terms of their overall approaches before exploring how their authentication mechanisms involve browser based activity, smartcards, mobile devices and biometrics.

### Dimension 2.1: DI Platform

As discussed in Dimension 1.1: National identity infrastructure, there are several models for the way in which a country will approach identity. When it comes to implementing DI many countries follow the same model of creating a national platform. In 77% of the countries there is a central entity responsible for providing authentication but also in developing, supporting, securing and sharing components and code that ensure interoperability between DI providers and public services.

Figure 2.11. Features of national DI platforms



*Source:* Based on information provided by Austria, Canada, Denmark, Estonia, India, Italy, Korea, New Zealand, Norway, Portugal, Spain, United Kingdom and Uruguay in response to the OECD survey Benchmarking Digital Identity Solutions (Unpublished).

Using DI to provide **additional attributes** expands the scope beyond authentication or a signature. This allows a citizen to obtain specific data, play a legal role, or prove a professional skill or responsibility. In addition to the authentication process, 23% of the selected countries use DI to provide access to attributes including tax information, address, birthdate, and professional information.

15% of the selected countries enable individuals to digitally sign documents on the basis of a role they hold. For example, in **Portugal** it is possible to use existing authentication mechanisms (Mobile ID and ID card) to access additional attributes and to take on the legal

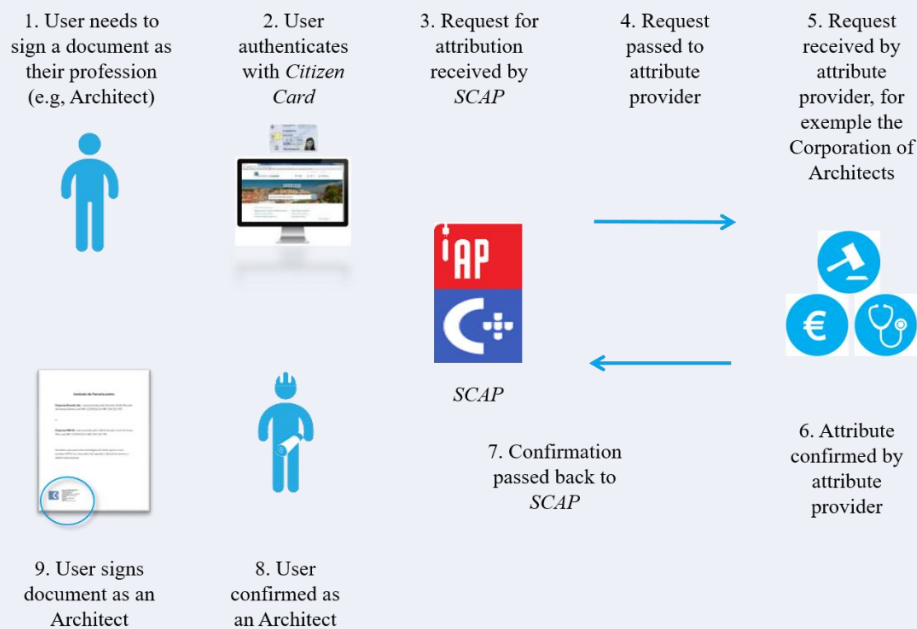
responsibility of another individual. The Portuguese Professional Attribute Certification System Case Study is considered in more detail in Box 2.5.

### Box 2.5. Portuguese Professional Attribute Certification System

Portugal's Professional Attribute Certification System (*SCAP*) uses existing, non-digital, authentication mechanisms to enable citizens to be authenticated according to the functions and entitlements they hold as a qualified professional.

*SCAP* ensures interoperability between existing identity mechanisms and attribute providers in order to support the authentication and the digital signing of documents according to the different roles citizens have.

Figure 2.12. *SCAP* functional architecture



Through the association of business attributes with their identity *SCAP* allows a citizen to use their Citizen Card or Mobile ID to authenticate and provide signatures as a legally recognised actor, such as Managers, Administrators, and Directors.

*SCAP* is also used internally by public servants to authenticate and electronically sign documents, according to the role of “public servant”.

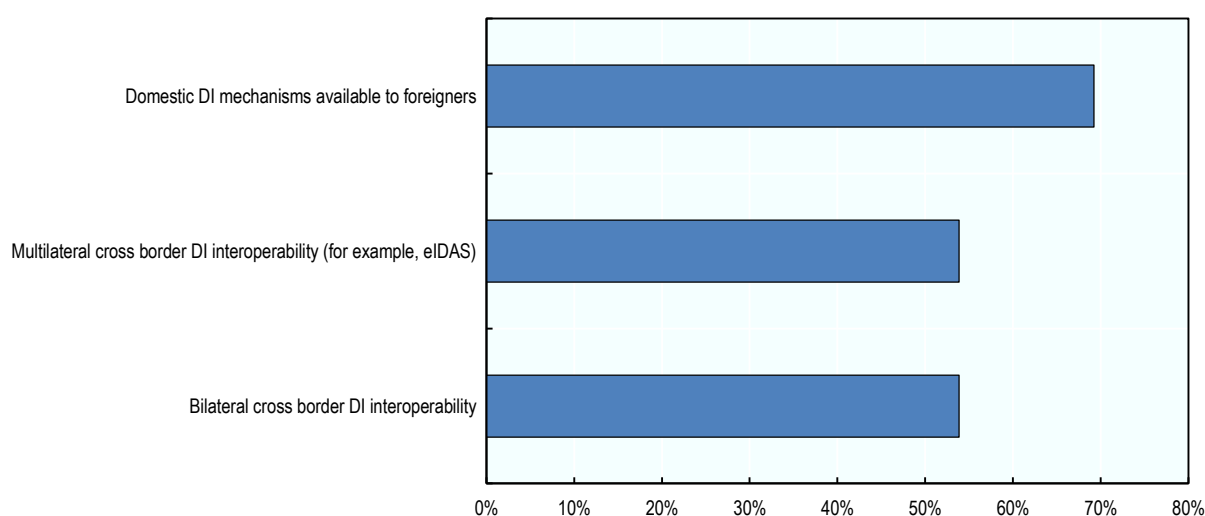
Figure 2.13. Main steps in the *SCAP* user journey for electronic signatures



Source: Portuguese Government Agência para a Modernização Administrativa (2018<sup>[3]</sup>)

Certain DI approaches enable countries to provide **cross-border** services and their citizens to identify themselves when accessing the services of another country. Nearly 70% of countries provide similar DI mechanisms for both national, and foreign, citizens. Additionally, over half of the countries have bilateral agreements which allow citizens to use their national identification solutions to access public services outside their country of origin. Finally, the implementation of European Regulation 910/2014, commonly known as eIDAS, amongst the EU member states means that **Austria, Denmark, Estonia, Italy, Norway, Portugal, and Spain** are covered by an expectation to deliver international cross border DI using a common interoperability solution.

**Figure 2.14. Cross-border DI**

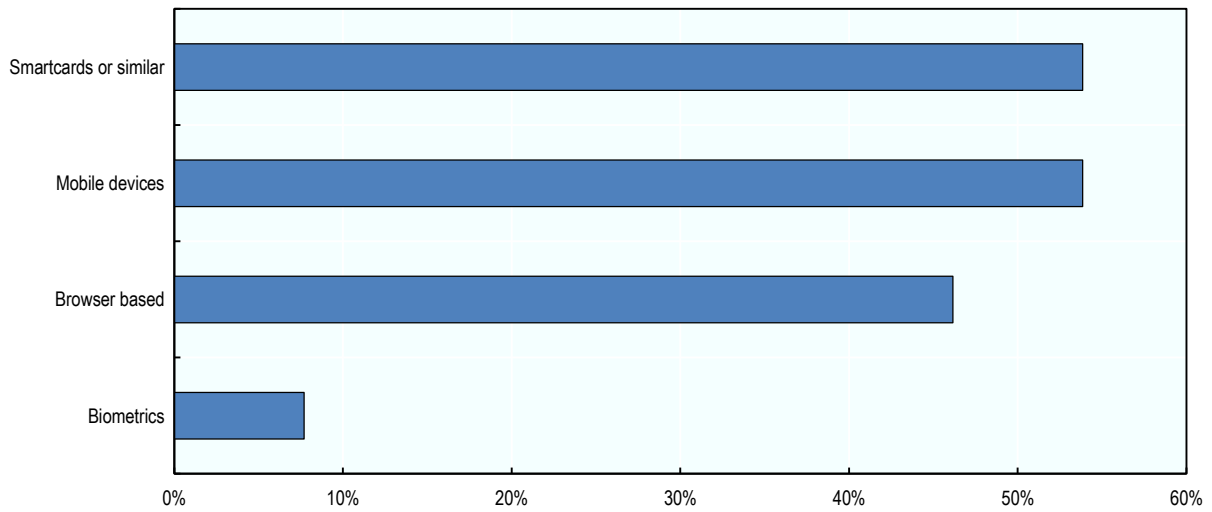


*Source:* Based on information provided by Austria, Canada, Denmark, Estonia, India, Italy, Korea, New Zealand, Norway, Portugal, Spain, United Kingdom and Uruguay in response to the OECD survey Benchmarking Digital Identity Solutions (Unpublished).

Some countries are making DI available not just to those who live in their country, but to anyone who wishes to have a government backed identity regardless of their residency. A particularly interesting example is that found in **Estonia**; their e-Residency project, discussed in Dimension 4: Transparency and monitoring, allows a DI to be requested by any citizen in the world.

Figure 2.15. Means of authentication within DI solutions explores some of the decisions countries have taken in implementing DI. Smartcards, or another physical second factor, form part of the solution in 7 of the countries; mobile devices are used in a further 7 and are commonly associated with an increased likelihood of adoption (OECD 2018). Browser based authentication features in 6 countries with biometric authentication being employed by a single country.

**Figure 2.15. Means of authentication within DI solutions**

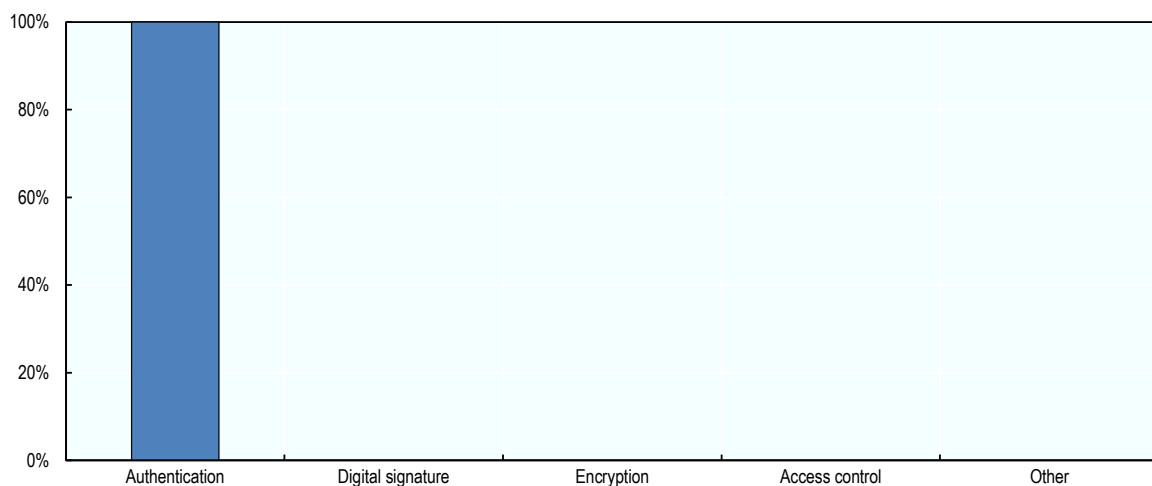


*Source:* Based on information provided by Austria, Canada, Denmark, Estonia, India, Italy, Korea, New Zealand, Norway, Portugal, Spain, United Kingdom and Uruguay in response to the OECD survey Benchmarking Digital Identity Solutions (Unpublished).

### *Dimension 2.2: Browser based*

Browser based approaches to DI are found in 6 of the countries featured in this study (**Canada, India, Italy, New Zealand, United Kingdom, and Uruguay**). This mechanism provides authentication only and is based on a user identifier and a password. These are often user defined but may reference an existing ID number, such as that found on an ID card, or involve a pre-set password. They may be paired with a second factor authentication step. The example of **Italy** is discussed in Box 2.6.

**Figure 2.16. Features of browser based DI**



*Source:* Based on information provided by Canada, India, Italy, New Zealand, United Kingdom and Uruguay in response to the OECD survey Benchmarking Digital Identity Solutions (Unpublished).

**Box 2.6. The Italian Public Digital Identity System (*SPID*) and Electronic Identity Card (*CIE*)**

The Italian Public Digital Identity System (*SPID*) enables Italian citizens to access online government services through a single DI (username and password).

*SPID* allows public administrations to replace their locally-managed authentication services with substantial savings in processing time and administrative costs. Moreover, compared to these legacy approaches, *SPID* increases the level of assurance as to whether the other party is who they claim to be..

*SPID* meets the requirements for assurance level “Low”, “Substantial” and “High” in line with the requirements of Article 7, Articles 8(1)-(2) and 12(1) of the eIDAS Regulation and Commission Implementing Regulation (EU) 2015/1502. As for the Low level see [https://www.agid.gov.it/sites/default/files/repository\\_files/documentazione/spid-avviso-n4-livelli-servizio-minimo-funz-omogenee.pdf](https://www.agid.gov.it/sites/default/files/repository_files/documentazione/spid-avviso-n4-livelli-servizio-minimo-funz-omogenee.pdf).

Art. 64 of the Codice Amministrazione Digitale - Digital Administration Code (CAD) provides that *SPID* is mandatory and that all government services should replace any previous authentication models with the exception of Electronic Identity Card (*CIE*). In order to speed up the process, simple instructions are provided at <https://developers.italia.it/en/spid>.

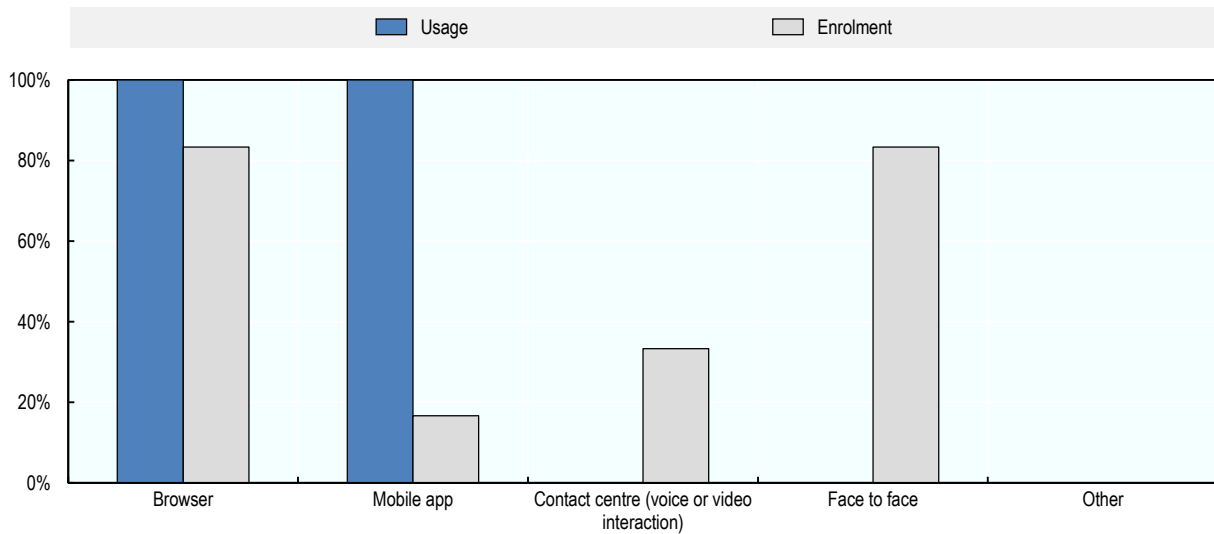
*SPID* has been recognized eIDAS compliant on Sept. 10, 2018 (<https://ec.europa.eu/cefdigital/wiki/display/EIDCOMMUNITY/Italy+-+SPID>).

*CIE* is both a personal identification document that certifies the identity of the holder and a means of authentication for online e-Government services. It aims to streamline and speed up communication between the state and citizens. The use of *CIE* is based on the cryptographic services installed on the card itself, and the interaction with the user device based on NFC. <https://www.cartaidentita.interno.gov.it/identificazione-digitale/entra-con-cie/>

*CIE* is a credit card that replaces the old paper-based ID document and former eID card. It is available to all Italian citizens. Through *CIE*, a citizen can obtain *SPID* online or in person. *CIE* has been recognized eIDAS compliant on Jun. 06 2019 (<https://ec.europa.eu/cefdigital/wiki/display/EIDCOMMUNITY/Italy+-+eID>).

*Source:* Provided by Italy in response to the OECD survey Benchmarking Digital Identity Solutions (Unpublished).

**Figure 2.17. Usage and enrolment channels for browser based DI**



*Source:* Based on information provided by Canada, India, Italy, New Zealand, United Kingdom and Uruguay in response to the OECD survey Benchmarking Digital Identity Solutions (Unpublished).

The countries adopting browser based approaches are focused on its use online and within mobile apps to provide authentication only.

Users can enrol across a range of channels with more than 80% of countries offering a face to face process whilst contact centres using video calls and the provision of mobile apps are additional channels designed to support an increased ease of enrolment.

Assuming that the mechanism for proving an identity has been solved, browser based DI is easy and cost-effective to implement with a positive user experience that can be readily replicated across multiple services. Efforts in **Italy** and the **United Kingdom** have focused on providing support to developers in service teams to simplify the work required to implement their approaches and reduce the adoption costs. For the user, there are no costs to bear in acquiring a DI and no costs when they use it.

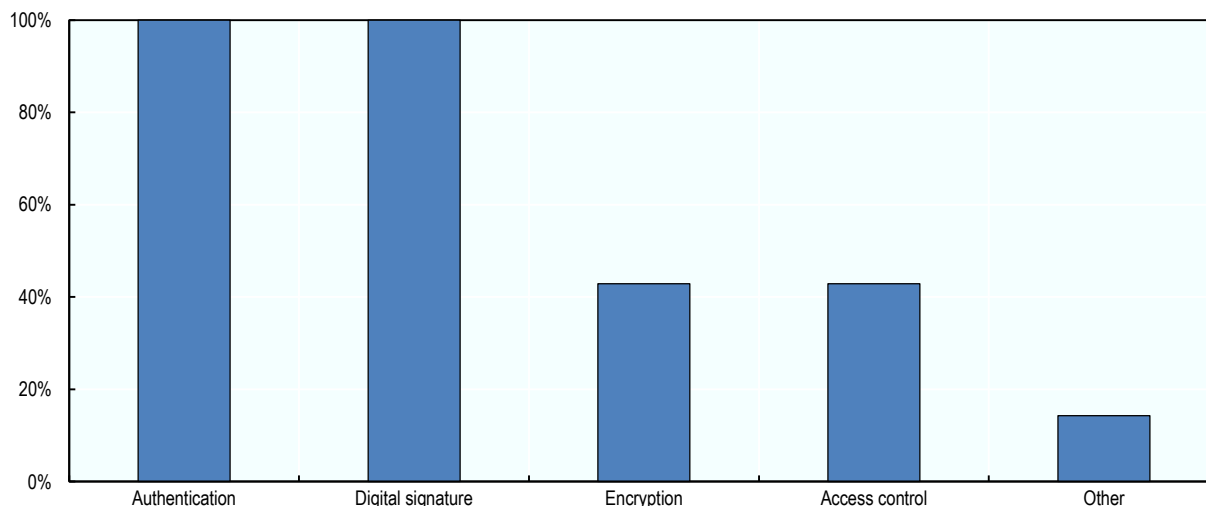
However, browser based mechanisms that only use a single factor of authentication are at risk of digital security threats such as phishing and do not provide some additional features such as digital signatures or encryption. To increase security when using a username and password, a second factor of authentication is recommended to ensure access is being granted to a legitimate party.

In **Italy**, in most cases, in order to increase the level of security, the browser based authentication requires SPID level “Substantial” which calls for second authentication factor. To protect high-value data or services, the level “High”, which requires mandatory asymmetric cryptographic keys besides second authentication factor.



### Dimension 2.3: Smartcards

Figure 2.18. Features of Smartcard DI



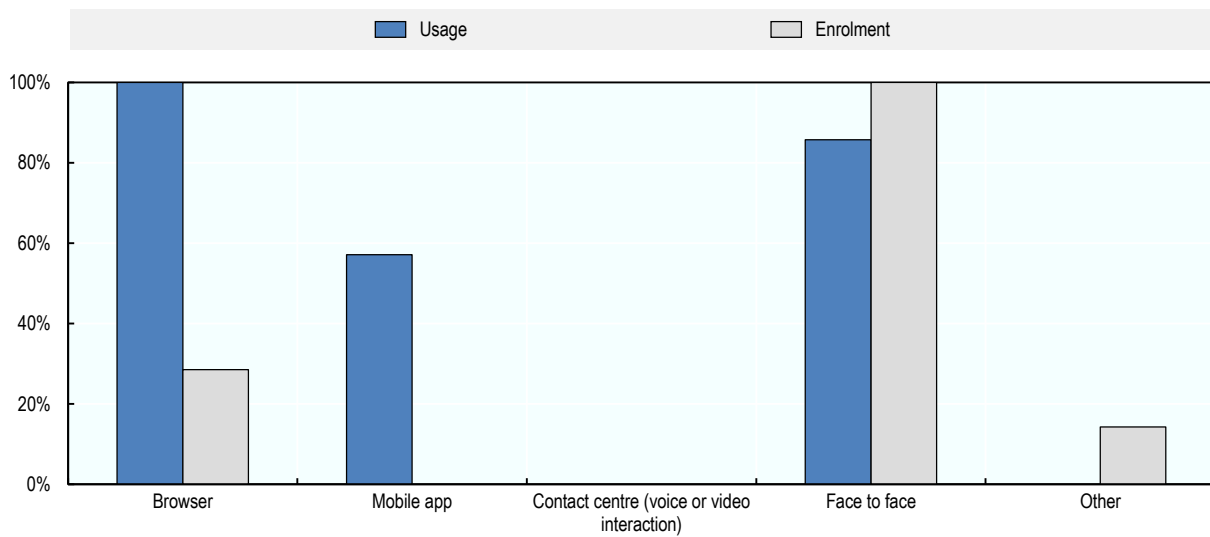
Source: Based on information provided by Austria, Denmark, Estonia, Korea, Portugal, Spain and Uruguay in response to the OECD survey Benchmarking Digital Identity Solutions (Unpublished).

Smartcards can form one element of the DI solution as seen in **Austria, Denmark, Estonia, Italy, Korea, Portugal, Spain, and Uruguay**. In all but one of these countries this second factor for authentication is provided through contact or contactless Smartcard technology. In **Denmark** the two factor solution is a code card (*NemID*).

The card based approaches of these countries provide a second factor authentication mechanism for online services and secure digital signatures. In addition, **Estonia** (see Box 2.11), **Spain**, and **Uruguay**, use Smartcards equipped with contactless technologies like Near-field Communication (NFC) or Radio-frequency identification (RFID) to manage permissions around access in the physical (real) world (including access to public buildings, public transportation, and airports). A further three countries have deployed Match on Card (MoC) Smartcard based solutions that reference fingerprint data in order to verify that the user enrolling for the card is who they claim to be. Finally, Smartcard implementations support encryption in some countries.

Smartcards are mostly used online or through face to face channels. Only those Smartcards which feature contactless technology are used to support mobile authentication. Users are always able to enrol for the use of Smartcards through face to face channels. **Denmark** supports online applications, **Portugal** supports online renewals, and **Estonia** allows people to register for their Smartcard by post.

Figure 2.19. Usage and enrolment channels for Smartcard based DI



Source: Based on information provided by Austria, Denmark, Estonia, Korea, Portugal, Spain and Uruguay in response to the OECD survey Benchmarking Digital Identity Solutions (Unpublished).

The Smartcard approach to DI is popular amongst frequent users in **Austria, Estonia, Portugal and Spain**. In these countries Smartcards underpin the identity infrastructure for professionals who perform several digital signatures or secure authentications per day (for example health care professionals, lawyers, and public servants) and are therefore a feature of daily life. For those users that do not need to engage in those activities as frequently, mobile approaches are favoured. Smartcards represent a DI solution that is effective when targeted at niche users but present challenges for governments intending to use it to provide digital services to infrequent users.

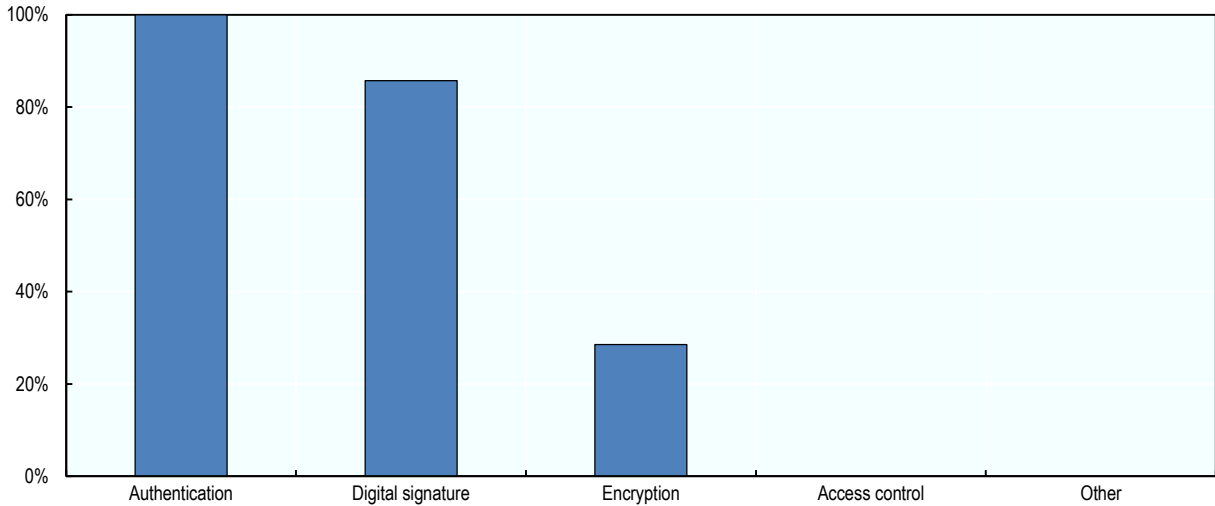
Smartcard technology brings with it greater costs than some of the other factors being considered. As well as the overhead of obtaining physical infrastructure to support their use, the item cost of a card is usually borne by a citizen. **Austria, Estonia, Portugal, Italy, Uruguay, and Spain** all charge for these cards at an average of EUR 24 for an adult, and often with subsidies for particular segments of the population.

Another important consideration for the design of Smartcards is how to approach the topic of validity. If a card contains biometric information relating to how someone looks then the card will need to be renewed after a period of time. However, the need to secure your Smartcard and the certificates that support it may require a shortening of the previously expected length of validity, or conversely enable countries to keep cards in circulation for longer than they might otherwise. In **Estonia**, the validity of the card and the validity of the certificate is 5 years meaning that renewal periods are synchronised. In **Italy** the validity of CIE is 10 years for individuals of age eighteen or above.



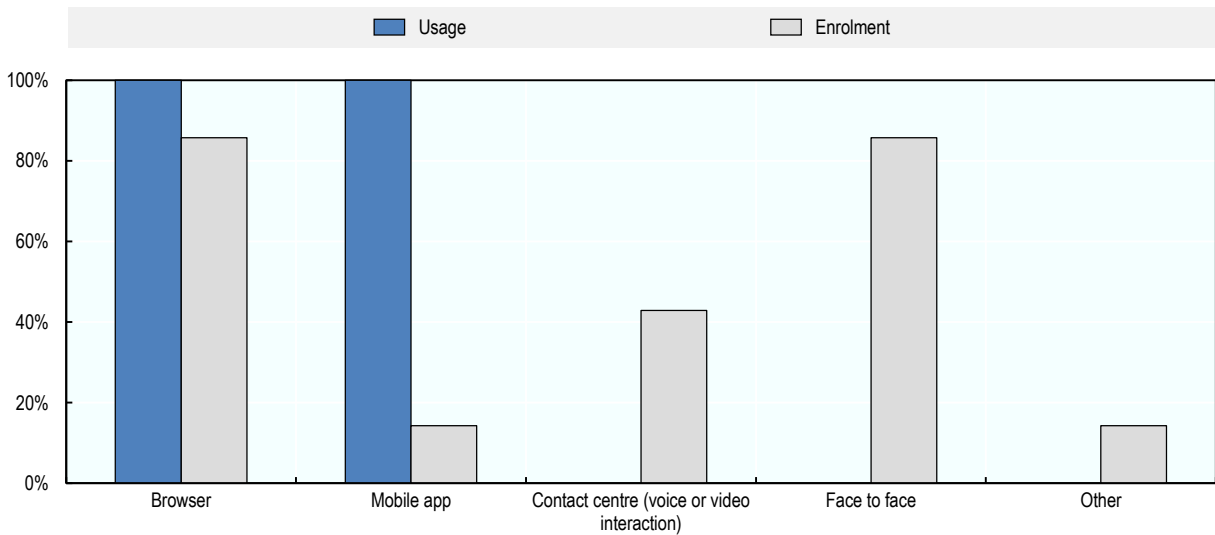
case of **Austria**, where the addition of a mobile user experience has increased adoption compared to the smartcard based process that had previously struggled to gain traction.

**Figure 2.21. Features of mobile DI**



*Source:* Based on information provided by Austria, Estonia, Italy, Norway, Portugal, Spain and the United Kingdom in response to the OECD survey Benchmarking Digital Identity Solutions (Unpublished).

**Figure 2.22. Mobile DI usage channels and enrolment process**



*Source:* Based on information provided by Austria, Estonia, Italy, Norway, Portugal, Spain and the United Kingdom in response to the OECD survey Benchmarking Digital Identity Solutions (Unpublished).

The countries using mobile devices are mainly focused on use online and within mobile apps. Users are usually able to enrol the use of their mobile devices through a face to face process or online, although this may require the use of their national ID as a confirmation of their authenticity. Contact centres using video calls and the provision of mobile apps are

additional channels designed to support the increased ease of enrolment. In **Estonia**, users must liaise with their mobile phone operator in order to upgrade their SIM card.

The use of mobile devices in support of DI approaches is increasingly common. For several countries, including **Austria**, **Estonia**, **Portugal**, and **Spain**, challenges with the user experience of Smartcards or security concerns around single factor authentication has motivated their use of mobile solutions. DI approaches that take advantage of mobile can offer an improved user experience, and enhanced security for accessing both government and private sector services.

Mobile DI approaches also provide the opportunity to simplify the application of more advanced functionality like digital signatures. In those countries where it is available, a mobile signature is the legal equivalent of a handwritten signature and can be used in any context without the requirement for additional hardware (unlike the use of a Smartcard). This is attractive both to infrequent users of the identity, and the providers of services themselves.

Using devices which citizens already have is an effective way of avoiding some of the implementation costs that might otherwise be required in providing Smartcards and encouraging adoption. Two factor authentication mechanisms using OTP sent by SMS or generated by existing authentication apps require little upfront investment by governments and add marginal costs to the provision of DI solutions. However, before considering the development of standalone mobile applications to support DI efforts countries should have confidence that the benefits it will produce will offset the ongoing overheads or challenges around introducing an additional step in adoption for users.

### Box 2.8 Mobile signatures in Austria


In Austria the development of a mobile device based signature solution has enabled the use of qualified electronic signatures in any location where a phone can be used. This simplifies the necessary software and hardware infrastructure compared to the former card-based approach.


The user experience is similar to that provided by banks for online banking. After successfully logging in with an access code and password, a code (referred to as TAN in Figure 2.23) is sent via text message to the associated mobile phone number. When this code is entered into the service, a qualified electronic signature is created.

Should users wish they can install an app on their phone to generate the required code instead of relying on text messages. An additional feature of the app is the ability to sign by simply scanning a QR code, removing the need to enter a code at all. It is anticipated that these app based interactions will replace text messages in most cases, particularly as the cryptographic relationship between the app and the device increases the level of security associated with the signature created in this way.

Due to the user friendliness and continuous development of this approach Austria sees more than 10 000 mobile phone activations per month and at the end of 2017 had more than 870 000 total users (approximately 10% of Austria's population).

Figure 2.23. Austrian mobile signature solution


Einfach elektronisch ausweisen und unterschreiben: Egal wann, egal wo 



**1. Schritt:**


- Die Signaturanfrage wird gestartet.
- Geben Sie Ihre Handy-Nummer und Ihr Signaturpasswort ein.

Mit der Handy-Signatur App können Sie zwischen TAN-Empfang mittels App oder QR-Code wählen:




**2. Schritt: TAN-Empfang**

- Sie erhalten eine TAN (Transaktionsnummer). Diese ist fünf Minuten gültig.



**2. Schritt mit QR-Code**

- »speed-sign«: Erfassen Sie den QR-Code am Bildschirm mit Ihrer Kamera am Mobiltelefon – und fertig.



**3. Schritt**

- Geben Sie die TAN ein
- Klicken Sie »Signieren« an und fertig.

**Hinweis:** Durch Klick auf »Signaturdaten« im Browserfenster bzw. »Dokumente anzeigen« in der App können Sie die Daten, die Sie unterschreiben, nochmals kontrollieren.

Source: Digital Austria (Austrian Government Federal Chancellery, 2017<sup>[1]</sup>)

### *Dimension 2.5: Biometric and emerging DI*

As seen in the case of **Spain** (Box 2.7) the increasing functionality of technology offers opportunities to revisit decisions about identity mechanisms. One of the most interesting emerging themes in identity relates to biometric data. Such data can provide a strong link between an ID card, an ID system, the data recorded in that system, the DI, and the citizen. Biometric data are often used by police and security forces to verify the citizen's identity but **India** is also using it to provide public services, their experience is discussed in Box 2.9.

Where biometric data are collected it most commonly incorporates a photograph; several countries also collect fingerprints. In **Portugal, Spain, and Uruguay** these data are held on the card and accessed using Match on Card technology. In **India**, biometric data are recorded in a central database and includes not only photograph and fingerprints but a scan of a user's eyes too which form part of the authentication process when a user attempts to access an Aadhaar enabled service.

Wider application of biometrics, for example in voice recognition or a heartbeat remain at the experimental, science fiction, end of the spectrum and were not present in any of the countries surveyed. Nevertheless, with smart home devices featuring voice matching and biometric data being used in schools to access pre-loaded credit for buying meals there is an increasing acceptance of these interactions as part of twenty first century life. Therefore, although only **India** has a DI approach where the biometric data forms part of each authentication, ongoing developments in smartphone technology will continue to improve the quality of cameras and immediacy of access to fingerprint scanners making it increasingly likely to feature in future approaches to DI.

Another trend that is indicated by the experience of several countries in this study is that of 'Bring Your Own Identity'. Users are increasingly familiar with the simplicity of reusing their credentials for email or social media to access other online communities or services. However, whilst simple to use, these methods are neither sufficiently trusted by users to protect their privacy or acceptable to businesses or government for providing the necessary assurance to transact as securely as possible. Consequently, governments and businesses, most notably **Canada, Denmark, New Zealand, Norway** and the **United Kingdom** are exploring how to establish trust based, but federated models of identity, that can reduce their overheads in managing and providing identity whilst enabling their users to increasingly access transformed digital services that can replace the need for face to face interactions.

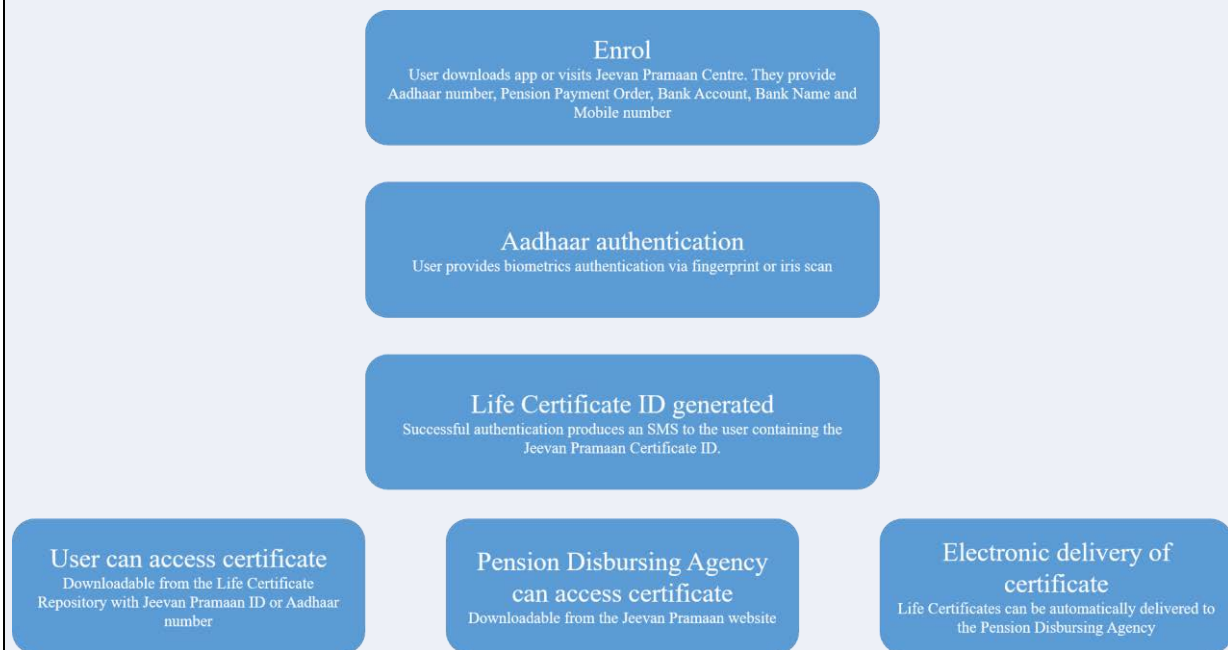
### Box 2.9. Aadhaar: the world's largest biometric ID system

With over 1.2 billion users, Aadhaar is the world's largest biometric ID system. Aadhaar relies on a 12-digit unique number issued to all Indian residents which is based on demographic and biometric data including photograph, ten fingerprints and scans of both eyes which are stored in a centralised database.

The Aadhaar card is printed on paper and is therefore not in itself a secure document, Security is instead provided by the use of biometrics which prevent the same person from enrolling a second time, with a different ID number. When a user wishes to access government services they do so with their Aadhaar identifier and either a fingerprint or eye scan.

One example of a service enabled by Aadhaar is the *Jeevan Pramaan* (Digital Life Certificate). After retirement, pensioners must provide Life Certificates to the relevant authorities but in order to get a Life Certificate, a citizen must personally present themselves before the relevant organisation. Through the *Jeevan Pramaan*, the Indian government are attempting to digitise the entire process, thereby making it possible to receive the certificate without having to attend in person. This will reduce unnecessary logistical hurdles and simplify the process for both citizens and the government.

Figure 2.24. Digital Life Certificate for Pensioners process



Source: Jeevan Pramaan, (2018<sup>[5]</sup>)

## Dimension 3: Policy levers and adoption

DI is fundamental to the digital transformation ambitions of countries wishing to embrace the breadth of opportunity offered by a digital government approach. This section on policy levers will discuss the legal and regulatory frameworks used by countries as well as the

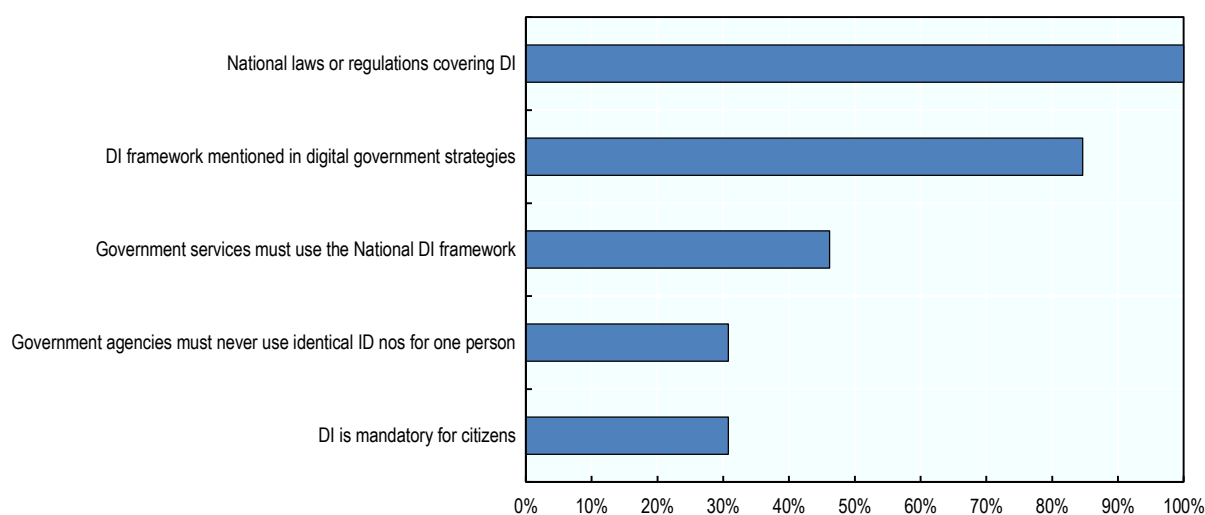


funding incentives, and enforcement deterrents supporting the implementation of DI. This is followed by an analysis of how the DI ecosystem has supported the development of services provided by both government and private sectors. Finally the major enablers and constraints to DI adopted are discussed.

### *Dimension 3.1: Legal and regulatory framework*

All countries have national laws or regulations relating to DI with 85% of them also mentioning DI in their strategies for implementing digital government and reducing administrative burden in order to be more responsive the needs of their users. **Denmark, Estonia, Korea, Portugal, and the United Kingdom** enforce the use of the national DI framework for central or federal government services. In **Denmark, Estonia, Korea, and Portugal** DI is legally mandatory for citizens.

**Figure 2.25. Legal and regulatory framework for DI in countries**



*Source:* Based on information provided by Austria, Estonia, India, Italy, Korea, Portugal, Spain, and Uruguay in response to the OECD survey Benchmarking Digital Identity Solutions (Unpublished)

**Austria, Canada, New Zealand, and Portugal** have specific laws or regulations forbidding the use of the same identifier for an individual across all government agencies. The example of Austria's SourcePIN, discussed in Box 2.1, is one approach to disaggregating information about individuals so that only that which is necessary for a service to meet a need is ever stored. However, legislation is not always required for this approach to be taken. In countries with a federated model, such as the **United Kingdom**, the disassociation of an identity from the transaction means that only the identity information required by the service is transmitted, or in some cases confirmed without transferring anything.

For the European Union member states considered by this study the eIDAS regulation provides an important legal basis to the delivery of cross-border services and the easy movement of citizens from one jurisdiction to another within the single market. Established in EU Regulation 910/2014 of 23 July 2014 it has been providing the legal underpinnings to the conditions under which member states have developed and enhanced DI solutions that could be recognised by other countries and reused by their citizens to access services throughout the single market. From September 29 2018 any organisation delivering public

services in an EU member state must recognise electronic identification from all EU member states. Regulation (EU) No 910/2014 of the European Parliament and of the Council (23 July 2014) on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC provides that one year from the date of the Member State's notification of the electronic identification scheme, all Member States should mutually recognise the electronic identification means falling under the notified scheme to allow to ensure the cross-border interoperability of the public administration online services which are already available.

### *Dimension 3.2: Funding and Enforcement*

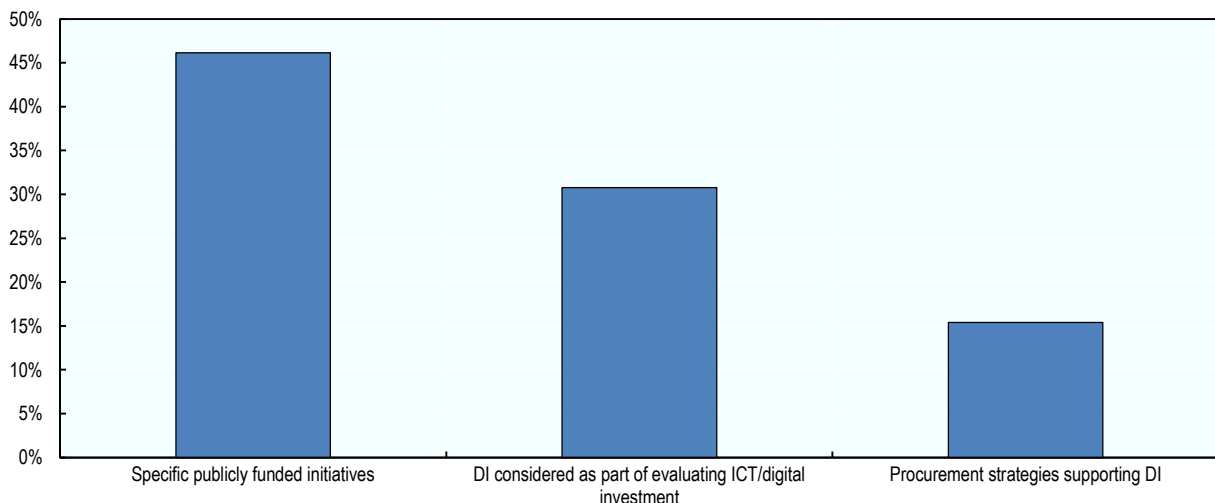
Nearly half of the surveyed countries have explicitly identified the use of public money to support the adoption of DI. In the **United Kingdom** this includes the funding of a common platform for others to reuse and centralised procurement of identity providers. In **Portugal**, all computers and laptops procured by public agencies have integrated smartcard readers to facilitate the dissemination of DI.

**Denmark, Portugal** (see Box 2.10), and the **United Kingdom** specify the adoption of DI as part of their evaluation of ICT/digital investment proposals from central or federal government departments and agencies.

Analysing business cases and evaluating procurement in light of DI policies is an effective complement to funding that encourages adoption. This is perhaps most clearly seen in the approach taken by countries to avoid charging their citizens for obtaining their original DI or replacing it.

Using funds to incentivise the development of a particular approach gives greater autonomy to service teams and government entities to meet the needs of their users whilst the process of evaluating ICT and digital spending can be seen as a more obstructive means of enforcing DI policy.

**Figure 2.26. Funding and enforcement to assist adoption of DI**



*Source:* Based on information provided by Austria, Estonia, India, Italy, Korea, Portugal, Spain, and Uruguay in response to the OECD survey Benchmarking Digital Identity Solutions (Unpublished)

### Box 2.10. Funding and enforcement of DI policy in Portugal

Portugal has a mandatory and binding ICT project and investment assessment process for all investment over EUR 10 000. The process adopts a multi-criteria assessment of investment with funds only being awarded to those projects which are successful assessed.

The process is the responsibility of the Agency for Administrative Modernisation (*Agência para a Modernização Administrativa, AMA*), who are also responsible for defining guidelines for digital government and has been important to the success of embedding DI policies. The process looks at the proposed return on the investment by analysing the total cost of ownership when set against the expected benefits. Whilst the financial aspect is important, all projects are considered in light of whether they align with existing government strategy and policies including those related to DI. Projects approved (or rejected) are published on a public dashboard with a merit system that rewards those agencies with the best ability to deliver.

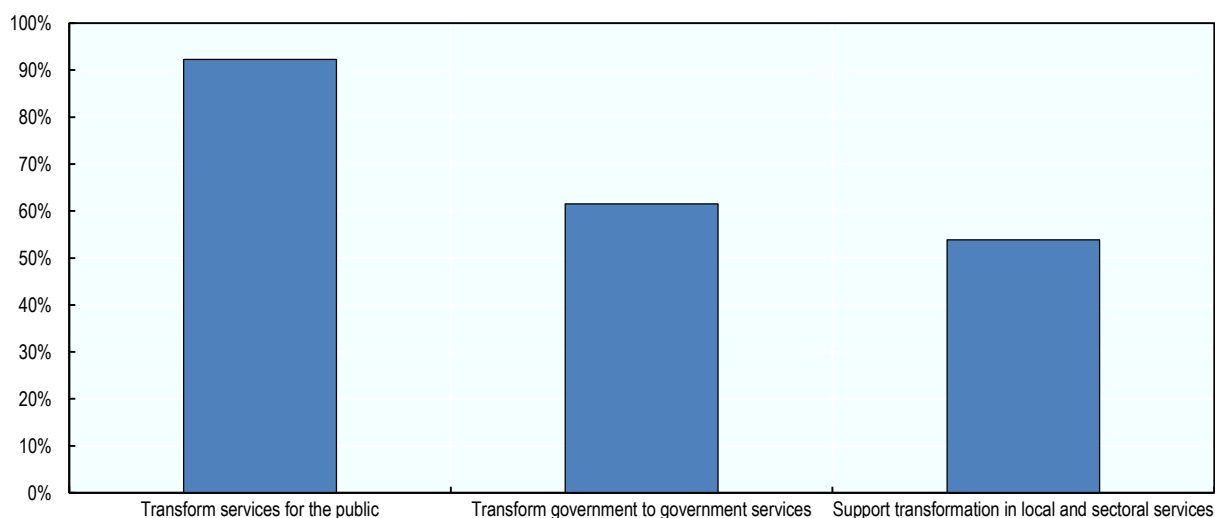
AMA is responsible for public funding programmes aimed at creating a simpler, more efficient and effective public administration focused on the needs of citizens and businesses. Agencies are able to request funding to improve their systems and services to reflect the national DI policy and platform.

These mechanisms of assessment and funding act as steering mechanisms to influence the focus, path and pace of delivery for DI and digital government in general.

*Source:* Provided by Portugal in response to the OECD survey Benchmarking Digital Identity Solutions (Unpublished).

### Dimension 3.3: Government services

Figure 2.27. The role of DI in transforming government services



*Source:* Based on information provided by Austria, Estonia, India, Italy, Korea, Portugal, Spain, and Uruguay in response to the OECD survey Benchmarking Digital Identity Solutions (Unpublished)

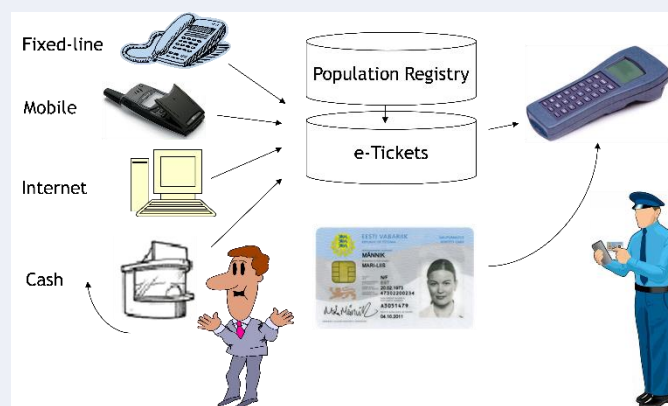
### Box 2.11. DI for public transport in Estonia

Some of Estonia's largest cities, Tallinn and Tartu, are using their identity infrastructure to provide 'virtual' tickets for travelling on public transport. Using their national ID cards citizens are able to buy tickets online, by SMS or at kiosks.

In order to use a virtual ticket customers must carry their ID card whilst travelling. During routine ticket checks users present this card, which is based on Smartcard technology, an inspector can read it and confirms the validity of the ticket.

The ticket details are not stored on the card but in a central database. The card is used by the ticket controller to lookup a record in the master database meaning the citizen need to only carry their ID card rather than any other form of ticket.

Figure 2.28. Estonian e-ticket flow



Source: Provided by Estonia in response to the OECD survey Benchmarking Digital Identity Solutions (Unpublished)

By being able to rely on a secure and effective DI, citizens are able to meet their needs without having to be physically present. The highest priorities for implementing DI were taxation, education and health. Whilst the primary focus of DI is initially central government services, more than half of the surveyed countries anticipate the adoption of DI within local governments and even in other channels. The example of **Estonia's** implementation across multiple channels is explored further in Box 2.11.

DI can also be an enabler of transformation for those working within government. Often overlooked by efforts to deliver more usable public facing services, public servants are being considered by more than half of the countries surveyed including **Denmark, Estonia, India, Korea, Norway, Portugal, Spain, and Uruguay**. In those countries DI is being applied to accounting and finance, public procurement, workflow for case management, administrative and managerial activity, legal functions.

#### *Dimension 3.4: Private sector services*

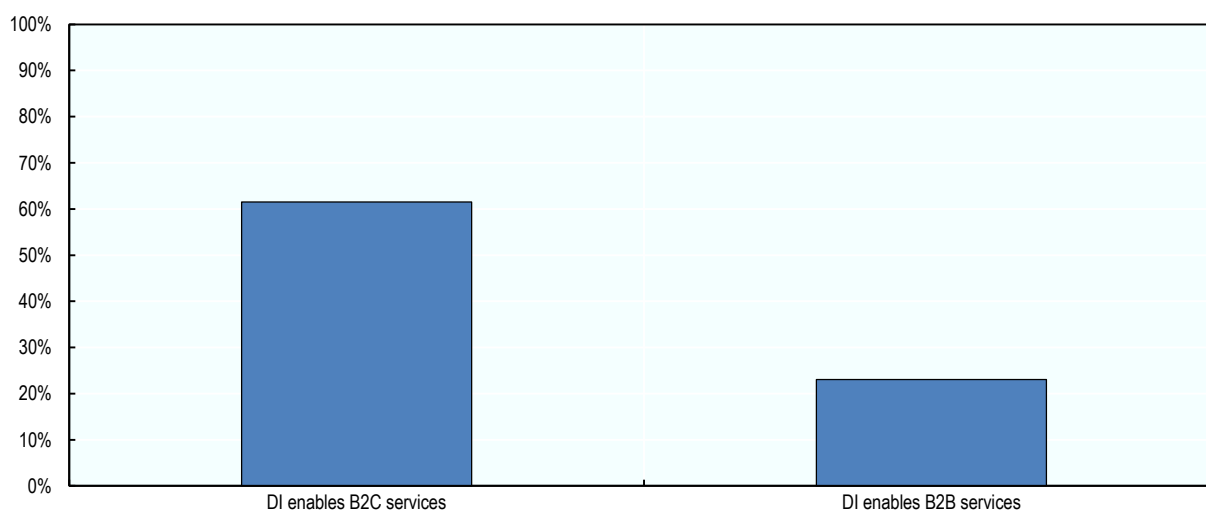
It is not only government that views DI as an important mechanism for benefiting from the opportunities of digital transformation. In **Austria, Denmark, Estonia, India, Italy, New Zealand, Norway, Spain, and the United Kingdom** DI is recognised as an enabler for Business to Consumer (B2C) services provided by the private sector. The reuse of **New**

**Zealand**'s RealMe DI by businesses is explored in Box 2.12. Three countries are using DI in providing Business to Business (B2B) services. **Austria, Estonia and Portugal** are working with businesses to implement DI in public procurement and electronic contracting.

The governance models for these countries is discussed in more detail in section 0 Dimension 1.3: Governance but whilst they reflect 4 of the 7 models between them, all of them involve the private sector in some way. In **Austria** and **Denmark** they have a shared DI model between the public and private sectors; **Estonia** has an model of interoperability with private or public sector DI usable for any service; **India**'s Aadhaar is a public DI designed for use by any service; **Norway** and the **United Kingdom** have DI models that use private sector identities; and **Italy, New Zealand, Portugal and Spain**, have public sector identities that can be reused by private sector services. This suggests that a private-public model of DI has broader benefits to a country's digital economy as the reuse of DI across sectors is mutually beneficial for government and the private sector too. In **Estonia**, the government estimates that the benefit of DI from B2C and B2B transactions (not government services) has been a 2% contribution to the national Gross Domestic Product (GDP) (OECD, 2018). Moreover, the experience of **Estonia** where only 17% of transactions requiring the use of DI are provided by public sector organisations, demonstrates the importance of creating the conditions under which public sector DI infrastructure can partner with the private sector to encourage adoption amongst the population by embedding DI into the everyday lives of citizens.

Approaches to DI that encourage its use by both government and private sector services are increasing both visibility, and familiarity. This amplifies the relevance of a DI mechanism as citizens use it more regularly than if they were solely limited to its application for public sector services. The reusability and interoperability of a given DI for accessing both government and private sector services adds value to citizens who don't need to manage multiple credentials or constantly create new accounts to prove who they are, and provides an additional incentive for uptake.

**Figure 2.29. The role of DI in transforming private sector services**

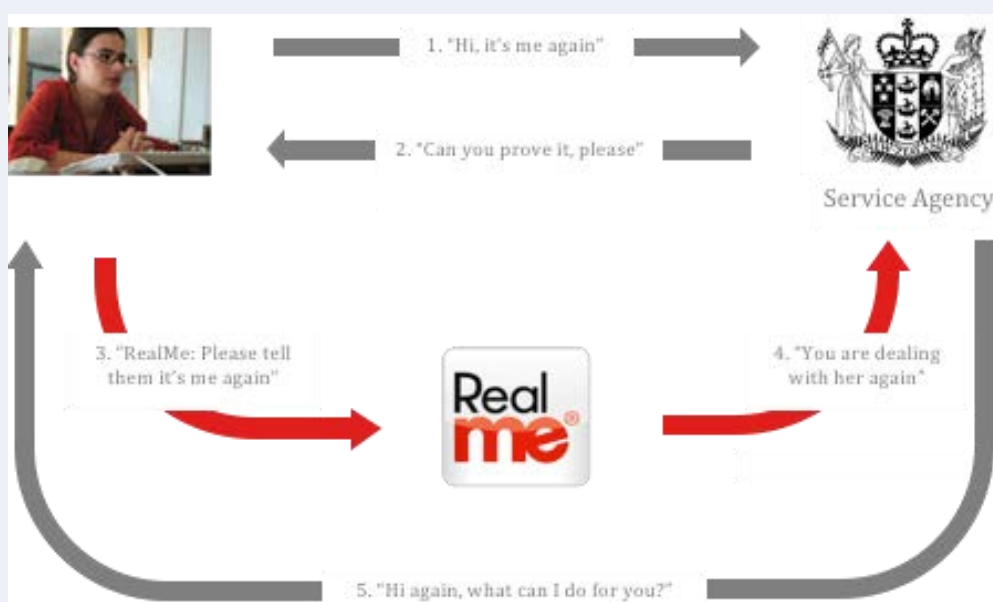


*Source:* Based on information provided by Austria, Canada, Denmark, Estonia, India, Italy, Korea, New Zealand, Norway, Portugal, Spain, United Kingdom and Uruguay in response to the OECD survey Benchmarking Digital Identity Solutions (Unpublished)

### Box 2.12. RealMe in New Zealand

The RealMe scheme allows citizens to access multiple government services with the same username and password. Users wanting to access a service are handed to the RealMe platform as part of their journey and after authentication, handed back to the service. RealMe stores no information but simply validates that a user can access a service, the individual retains control over what information they share and when they share it.

Figure 2.30. RealMe



The RealMe service was developed in partnership by the Department of Internal Affairs and the New Zealand Post. It responds to the needs of government whilst also proving used to the private sector. Users can use it for a range of services including opening a bank account, enrolling to vote, transferring foreign currency, applying for a loan or allowance, and renewing their passport online.

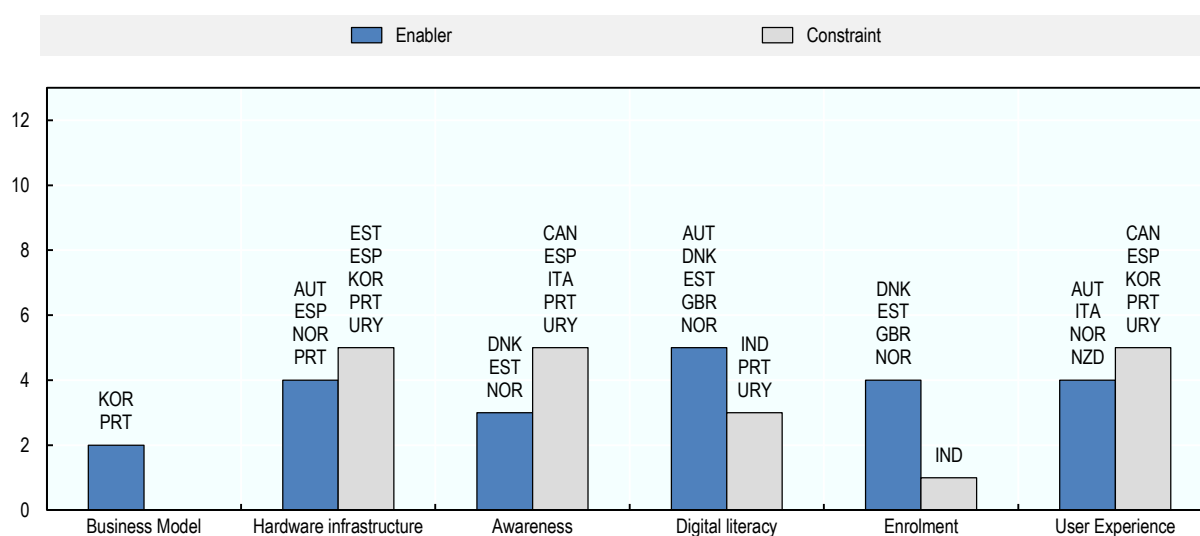
Source: Provided by New Zealand in response to the OECD survey Benchmarking Digital Identity Solutions (Unpublished).

### Dimension 3.5: Enablers and constraints

The experience of implementing DI in the surveyed countries identified areas of activity that have enabled this activity and other issues which should be understood as constraints. The OECD framework has identified the following themes:

- the business model
- hardware infrastructure (for both citizens and service providers)
- levels of digital literacy and awareness of the DI approach in society
- the user experience of enrolling and using the DI

**Figure 2.31. Enablers and constraints impacting DI adoption**



*Source:* Based on information provided by Austria, Canada, Denmark, Estonia, India, Italy, Korea, New Zealand, Norway, Portugal, Spain, United Kingdom and Uruguay in response to the OECD survey Benchmarking Digital Identity Solutions (Unpublished)

As Figure 2.31 shows, almost all of these are seen both positively and negatively in the contribution they make towards adoption of DI. The exception to this is the **business model** underpinning the choice of DI implementation. For **Korea** and **Portugal** this is identified purely as a positive contributor to supporting adoption. One approach to the business model behind DI is to reduce, or even eliminate, the fees involved with accessing government services that might otherwise have taken place face to face. In **Korea**, citizens who use the digital channel instead of attending in person receive a financial incentive.

For **Austria, Norway, Portugal** and **Spain**, the role of **hardware infrastructure** was identified as being an important enabling factor. In particular it was recognised that if a DI solution can use the mobile devices which people already own then there are increased opportunities for adoption. However, on the service provision side, the requirement for hardware to be available in order to authenticate using a second factor, such as with Smartcard technology was cited as a constraint by **Estonia, Korea, Portugal, Spain** and **Uruguay**. Removing the need for hardware infrastructure, or reusing existing technology, removes both a cost barrier and a logistical challenge to adoption.

In 5 of the countries (**Canada, Italy, Portugal, Spain** and **Uruguay**) the lack of **awareness** amongst the public is cited as being one of the main constraints whilst **Denmark, Estonia** and **Norway** identify it as one of the areas that has been targeted to increase adoption. The role of an approach which is embraced by both public and private sectors is an opportunity to share responsibility for raising awareness. **Austria, Denmark, Estonia, Norway** and the **United Kingdom** recognise **digital literacy** has a role to play in complementing efforts to increase the awareness of a DI approach with **India, Portugal** and **Uruguay** finding that to be a constraint.

Assuming that people are aware of the DI approach and are given opportunities to use, one of the areas countries must consider is the usability of the DI service that has been designed. This process begins with the **enrolment** of users with **Denmark, Estonia, Norway** and the **United Kingdom** indicating that making sure that the DI registration process is online and



costs the user nothing should be priorities whilst **India**, perhaps in recognition of the greater complexity of a biometric based DI approach, considers that enrolment is a constraint

This necessarily extends to the **user experience** of the DI approach when accessing a service with **Austria, Italy, New Zealand** and **Norway** considering that to be an enabler, and **Canada, Korea, Portugal, Spain** and **Uruguay** seeing it as a constraint. The discussion around different DI solutions (see Dimension 2: DI Solutions) identified that browser and mobile device based approaches provide the best user experience and, assuming the presence of two-factor authentication, provide suitable levels of security. Moreover, the private sector's incorporation of DI into their services is a positive factor in ensuring that people are comfortable with the DI approach with user journeys that are focused on successful outcomes.

#### Box 2.13. Canadian identity management accelerators

The government of Canada has a roadmap for making DI real across all jurisdictions and service channels in the country. Underpinning that are five principles:

1. **Communication:** evolve the messaging from what has been developed to sharing why it's important and what is realised if done well.
2. **Develop the Pan-Canadian Trust Framework** as a foundational piece to moving identity management forward.
3. **Use Pilots** to test out the trust framework and support the delivery of citizen-centred services.
4. **Technology:** stay up to date with rapidly advancing technologies and ensure adoption does not preclude standards.
5. **Public Policy and Governance:** articulate a shared public policy position on identity management to help determine what governance structure and approval authorities make sense.

*Source:* Provided by Canada in response to the OECD survey Benchmarking Digital Identity Solutions (Unpublished).

## Dimension 4: Transparency and monitoring

The OECD Recommendation on Digital Government Strategies (OECD, 2014<sup>[6]</sup>) calls on governments to recognise the importance of Openness and Engagement in the following ways:

1. Openness, transparency and inclusiveness
2. Engagement and participation in a multi-actor context in policy making and service delivery
3. Creation of a data-driven culture
4. Protecting privacy and ensuring security

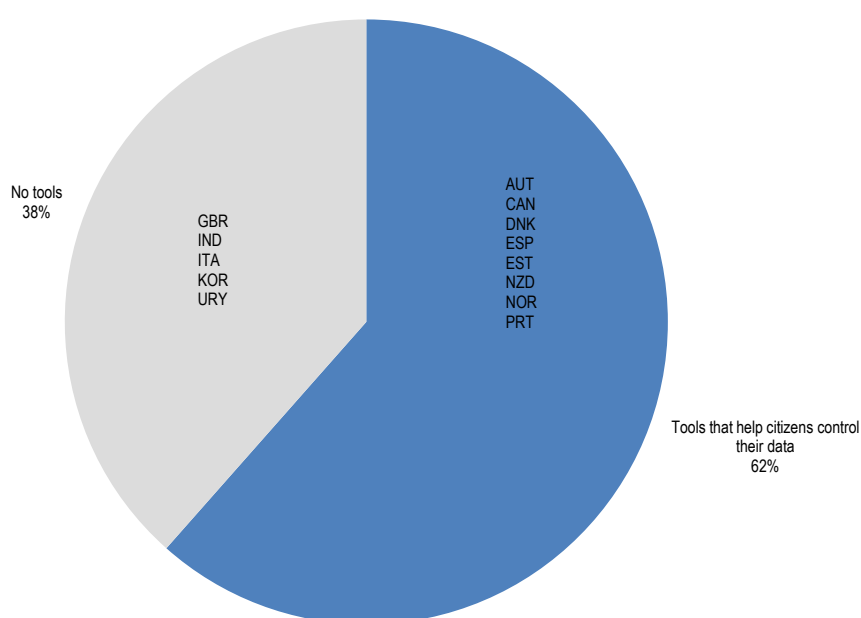
Given the importance to government of having confidence that they are engaging with the person they believe to be using the DI credentials, and in the public having confidence that government is treating their personal data with respect, these themes are highly relevant.



This section explores how countries are approaching this topic with regard to the ways in which users are being given control of their data, the data governments publish about DI performance, and the impact assessment and cost-benefit evaluation mechanisms in place to judge the success of the scheme.

Different countries are exploring how to put citizens in greater control of who can access their data, visibility of how that data are used and the power to revoke, refuse or consent to requests for access. Publishing performance data, especially as open data, allow stakeholders to track the level of use of DI mechanisms, and achieve near real time monitoring of its impact. Finally, the availability of impact assessment and cost-benefit evaluation mechanisms are important in assessing the maturity and effectiveness of DI policies and solutions.

**Figure 2.32. Provision of tools that help citizens control their data**



*Source:* Based on information provided by Austria, Canada, Denmark, Estonia, India, Italy, Korea, New Zealand, Norway, Portugal, Spain, United Kingdom and Uruguay in response to the OECD survey Benchmarking Digital Identity Solutions (Unpublished)

#### ***Dimension 4.1: Citizen control of their data***

The majority of the selected countries (62%) provide tools for citizens to see how their data are being used, and thereby increase their trust in DI systems.

One approach, which is being prioritised in the thinking around the future of DI in Chile, is to show users an audit of all activity on and around their account such as *Carpeta Ciudadana* in Spain (Box 2.14). This includes not just the logins performed by users but also the way in which organisations have used their data. In certain situations citizens are able to accept, or refuse, the re-use of their data.

In **Denmark**, anyone with a *NemID* can access a personal activity log which monitors all uses of the *NemID*. Citizens can opt out of having any log made, removing the record not just for themselves but for government too.

**Box 2.14. *Carpeta Ciudadana***

*Carpeta Ciudadana* enables a citizen to know and control access to their data by public organisations. It provides a summary of the citizen's information grouped by subject and displays the number of files currently open, or in the pipeline, at the time of their query, grouped by ministry or agency. It then links the user to further details about the files.

*Carpeta Ciudadana* shows information about the exchange of information between public organisations and the condition of consent placed upon it. The list of data that has been requested, and shared with, administrative bodies to complete a formality or query also displays whether the citizen has given explicit, or tacit, consent for its reuse.

*Carpeta Ciudadana* is not just focused on the DI experience of the citizen, additionally presenting logs of any face to face interactions between the citizen and the public administration.

*Source:* Provided by Spain in response to the OECD survey Benchmarking Digital Identity Solutions (Unpublished).

Another approach for increasing transparency favoured by several countries, and in the case of **Portugal** discussed in Box 2.15, is to request the explicit permission of the citizens to grant access to particular attributes within the authentication process.

### Box 2.15. *Autenticação.Gov*

In **Portugal**, *Autenticação.Gov* provides a central DI platform for securely authenticating users for public and private sector services. The platform supports Smartcards, mobile devices and additional browser based forms of authentication. The service provider judges the appropriate level of authentication required for the service being accessed and this restricts the DI mechanisms shown to the user. As an example, access to the Public Taxes Portal requires Level 3 authentication which is only available through Smartcard or mobile authentication whilst the Citizen Portal operates at Level 2 and has a lower set of requirements for authentication.

In terms of transparency, when a user authenticates (regardless of the mechanism they use) they are given control of the data attributes to be provided to the service provider. These data are subsequently retrieved from across government, digitally signed by government, and transferred to the service provider as part of a successful authentication.

**Figure 2.33. Citizen authorisation for sharing attributes when using *Autenticação.Gov***

**AUTENTICAÇÃO.GOV**

Faça a sua autenticação com :

CARTÃO DE CIDADÃO    CHAVE MÓVEL DIGITAL

Portal do Cidadão solicitou alguns dos seus dados para realizar o serviço *online* pretendido [7]

- Nome Próprio
- Apelido
- Data de Nascimento
- Nome Completo
- Identificação Fiscal
- Identificação Civil

} Authorised  
citizen  
attributes

**Método de autenticação**

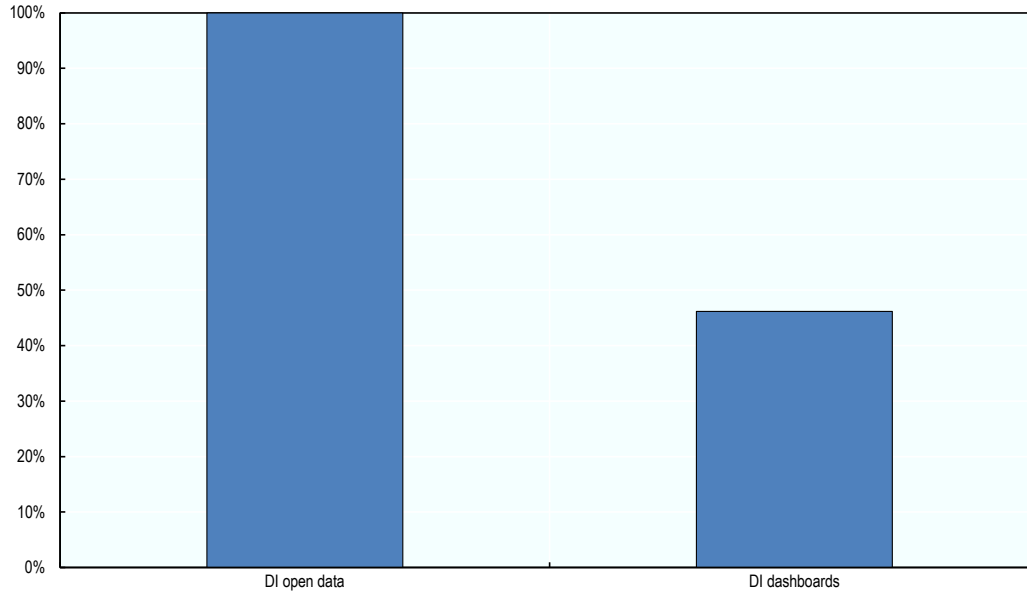
Telemóvel     Email     Twitter

RECUSAR    AUTORIZAR

*Source:* Provided by Portugal in response to the OECD survey Benchmarking Digital Identity Solutions (Unpublished).

### Dimension 4.2: Performance data

Figure 2.34. Availability of DI performance data



Source: Based on information provided by Austria, Canada, Denmark, Estonia, India, Italy, Korea, New Zealand, Norway, Portugal, Spain, United Kingdom and Uruguay in response to the OECD survey Benchmarking Digital Identity Solutions (Unpublished)

All the countries surveyed for this study publish open data about their DI performance whilst **Austria, Canada, Denmark, Estonia, Portugal, and the United Kingdom** also provide real-time, or near real-time, dashboards. This information allows stakeholders to track the level of use of DI.

In **Estonia**, the country's e-Residency scheme (Box 2.16) demonstrates not only an innovative approach to encouraging the adoption of DI by citizens of other countries around the world, but also in the level of transparency available in terms of its performance.

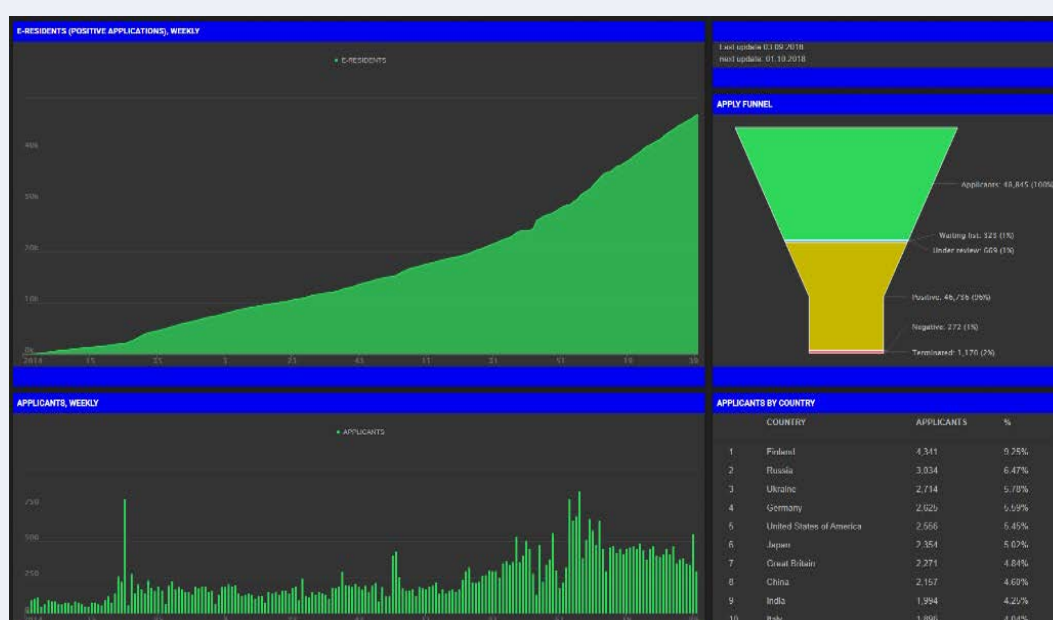
### Box 2.16. e-Residency in Estonia

**Estonia's** e-Residency scheme is a transnational DI for any non-Estonians and non-residents of Estonia in the world. It allows an individual to establish a location-independent online business in Estonia, with access to digital services similar to those accessible by Estonian citizens and Estonia-based businesses.

The vision is to provide secure and effective digital services for global citizens who are investors, entrepreneurs, students, freelancers, developers, and others. e-Residency is challenging the society to think about what it means to be global in the future and how to bring the world together – for individuals, businesses, and governments.

Importantly, e-Residency offers full transparency in the results and its progress through regularly updated, public dashboards.

Figure 2.35. e-Residency performance dashboard



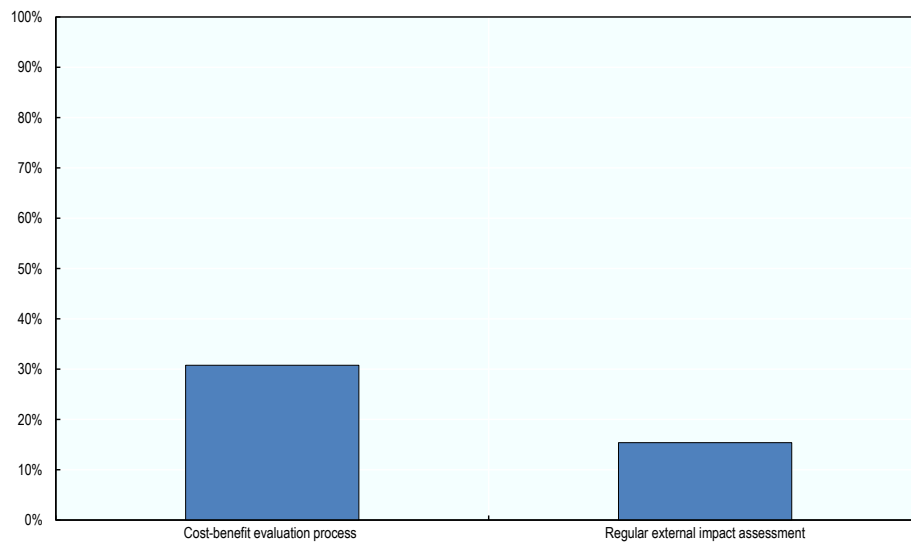
Source: Estonian e-Residency application dashboard (Estonian Government, 2018<sup>[77]</sup>)

### Dimension 4.3: Impact assessment

**Denmark, Portugal** (Box 2.10, **Spain** and the **United Kingdom** have processes in place to conduct cost-benefit evaluations of spending on ICT and digital projects in the context of DI policies. The situation found in each country means that the cost-benefit analysis from one country is not the same as that found in another, preventing more in-depth comparison of how these countries identified the appropriate mechanism for them.

**Canada** and **Portugal** also conduct regular external impact assessments of DI. These assessments are performed by external parties, including universities, to measure the effective impact of DI on the citizen, the economy, and in society. Moreover, in **Canada**, the National Management Accountability Framework reflects DI indicators (Box 2.17).

**Figure 2.36. How the impact of DI is assessed**

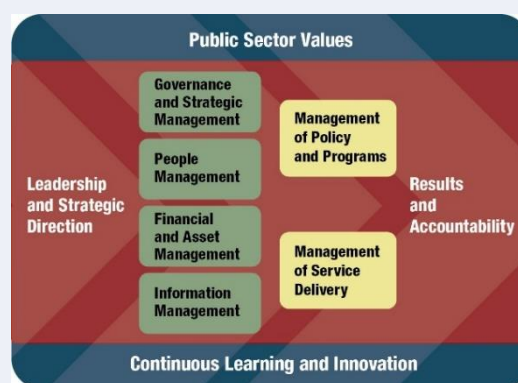


*Source:* Based on information provided by Austria, Canada, Denmark, Estonia, India, Italy, Korea, New Zealand, Norway, Portugal, Spain, United Kingdom and Uruguay in response to the OECD survey Benchmarking Digital Identity Solutions (Unpublished)

### Box 2.17. Assessing adoption of DI in Canada

**Canada's** Management Accountability Framework (MAF) requires departments to report on their progress against certain indicators, including those related to DI. Within MAF, departments must report on their progress in adopting Cyber Authentication services and compliance with the identity policy instruments.

**Figure 2.37. Canadian Management Accountability Framework**



*Source:* Canadian Management Accountability Framework, <https://www.canada.ca/en/treasury-board-secretariat/services/management-accountability-framework.html> (Canadian Government, 2017<sup>[8]</sup>),

## Observed trends

On the basis of the experiences discussed above nine trends present themselves:

### *Design DI for reuse*

The success of DI frameworks depends on the level of adoption and usage by citizens. Therefore, ensuring that services, which require strong confidence in the identity of a user, can use a single DI approach, regardless of whether they're delivered by the public or private sectors.

### *Focus on the user experience*

The user experience for DI is an important success factor. DI will not meet expectations for delivering results if the user experience fails to be well designed and is not immediately accessible to users by requiring the installation of specific software or the acquisition of additional hardware.

### *Digital literacy matters*

There is a correlation between adoption of DI and digital literacy in a population. Therefore, as well as ensuring that the approach to DI recognises the needs of those with lower digital literacy, activities to raise awareness, and develop digital skills are advised.

### *Go mobile*

The relentless growth of mobile internet access and smartphone ownership around the world makes it essential for the design and implementation of DI solutions to reflect the opportunities provided by mobile devices. Several of the countries discussed in this benchmarking exercise have had positive experiences with mobile DI solutions and are migrating from legacy approaches to a mobile first model.

### *Adopt open standards for interoperability*

When DI platforms support open standards (for example, SAML2 and OAuth2) they are more successfully adopted by services provided by both the public and private sectors. Open standards ensure independence from proprietary software providers and allow for more straightforward implementation by services, and facilitate interoperability with multiple authentication providers, even those supporting citizens in other countries.

### *Continuously improve the DI offer*

Approaches to DI can improve in response to developments in what's possible. This is seen in the increased use of mobile devices, and in those countries, which have used DI to design out the need for signatures. Elsewhere, countries have made it easier for services to implement their DI into existing provision and have made it easy to enable the sharing of professional attributes or using the same DI to operate in a legal capacity alongside using it personally.

### *One size does not fit all*

Countries are comfortable to offer different mechanisms to different sections of society. Whilst mobile devices increasingly form part of the landscape for the general population, the needs of professionals are often met by Smartcards. In countries where private sector

DI is available then its reuse by the public sector offers increased benefits to government whilst reducing the friction of adoption.

### *The 3 “S” of digital ID policy: Security, Signature, and Single sign-on*

National DI policies are focused on approaches that are secure, which allow for transforming the experience of signing documents and provide common, single, mechanisms for authentication.

### *The citizen is in control*

Giving a citizen control of their identity and their data are seen across this study. This includes:

- i) allowing the definition of **which attributes** can be made available to a service
- ii) providing **transparent tools** that give citizens visibility over the use of their data, and
- iii) publishing **open data** on how different approaches are performing.

## References

- Austrian Government Federal Chancellery (2017), *Digital Austria*, <https://www.digital.austria.gv.at>.
- Canadian Government (2017), *Canadian Management Accountability Framework*, <https://www.canada.ca/en/treasury-board-secretariat/services/management-accountability-framework.html>.
- Estonian Government (2018), *Estonian e-resident application dashboard*, <https://app.cyfe.com/dashboards/195223/5587fe4e52036102283711615553>.
- Jeevan Pramaan (2018), Jeevan Pramaan, <https://jeevanpramaan.gov.in>.
- MIDESO (2017), *Encuesta de Caracterización Socioeconómica Nacional*, Ministerio de Desarrollo Social de Chile.
- OECD (2014), *Recommendation of the Council on Digital Government Strategies*, [OECD/LEGAL/0406](https://www.oecd.org/LEGAL/0406).
- OECD/ITU (2011), *M-Government: Mobile Technologies for Responsive Governments and Connected Societies*, OECD Publishing, Paris, <https://dx.doi.org/10.1787/9789264118706-en>.
- Portuguese Government Agência para a Modernização Administrativa (2018), Portuguese Professional Attribute Certification System.
- UK Government (2018), *Guidance - GOV.UK Verify*, <https://www.gov.uk/government/publications/introducing-govuk-verify/introducing-govuk-verify> (accessed on 1 July 2108).



### 3. DI in Chile

*This chapter presents a summary of DI provision in Chile according to the framework explored in the preceding chapter.*

*The chapter starts by looking at the foundations for identity in Chile in terms of existing national identity infrastructure, the policies supporting DI and Chile's governance mechanisms.*

*In the second section, the existing model of DI in Chile is looked at in terms of its technical approach. The policy levers and adoption for Chile's DI are assessed in light of the legal and regulatory framework, funding and the enforcement measures, the services made available, and the enablers and constraints identified in Chile as well as the intentions around putting citizens in control of their data, the openness with which performance is being shared and the approach to assessing impact.*

*Finally, the chapter ends with the plans Chile have for expanding ClaveÚnica*

## DI in Chile

Chile is at a transition in terms of its approach to DI. Having built on the existing model of demonstrating identity with a physical card, the country launched ClaveÚnica in 2012. This mechanism for proving that someone is who they claim to be when accessing online services is now moving into a further development to extend its functionality and utility with the ambition that it becomes the default mechanism for people to access, and grant permission for access, to their records across the public and private sector. The functionality of ClaveÚnica is intended to allow for:

1. **Data authentication:** the mechanism by which citizens will be identified to access state services and other private organisations
2. **Data wallet:** A store of personal data for citizens which will allow interoperation with institutions on the basis of the access and re-use permissions which a citizen grants on their information
3. **Advanced electronic signature:** Users of ClaveÚnica will be able to sign electronic documents issued by public bodies
4. **Citizen mailbox:** A means by which the state will notify citizens of important information and progress on their interactions with the state
5. **Web portal eID:** a website where citizens can manage access to their data, grant and revoke permissions and update their personal data

This chapter will consider the situation in Chile in comparison to the benchmarked countries and provide a summary of both the ‘as is’ experience and the imagined future. This will provide the basis for the Assessment and Recommendations of this study.

## Foundations for DI in Chile

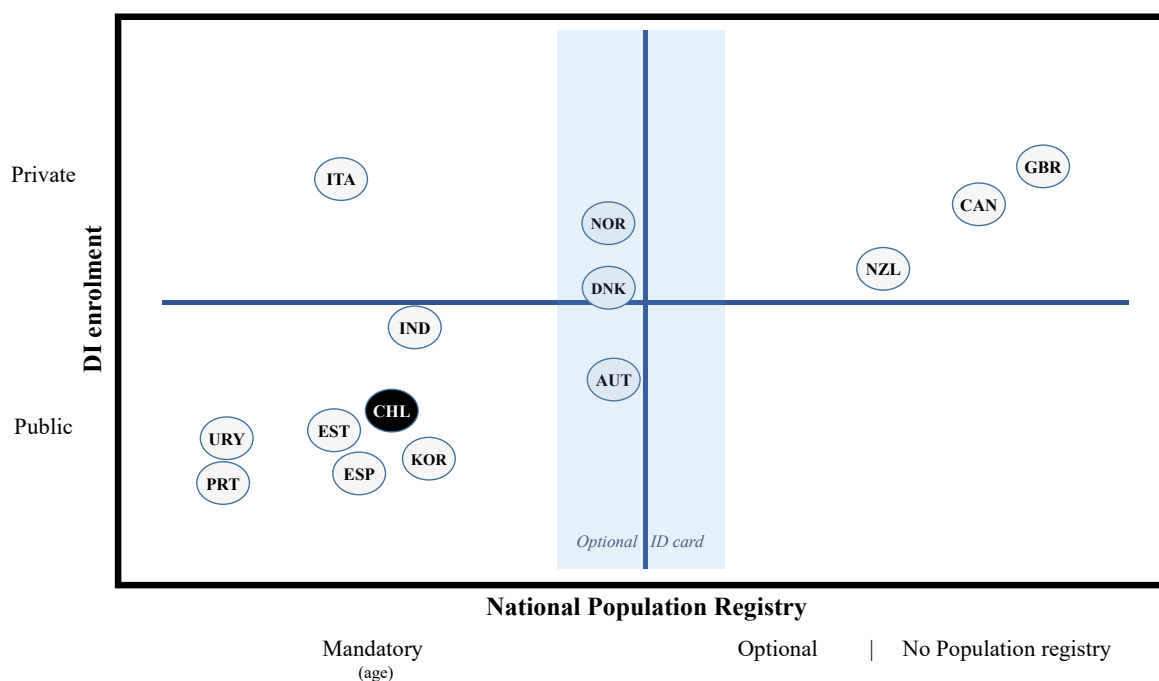
### *National identity infrastructure*

In Chile, the registration of all citizens, Chileans and immigrants, is administered by the Civil Registry Service of Chile (*Servicio de Registro Civil e Identificación*, SRCeI). The SRCeI issues a physical card, the *Cédula de Identidad*, which must be carried and is used by citizens travelling inside the country, proving identity at public and private institutions, and for voting. This publicly operated, centralised register of the population provides the basis for the way in which the country is approaching the question of DI. This model is the basis for several countries discussed in this study including **Austria, Estonia, India, Korea, Portugal, Spain, and Uruguay**.

To complement the physical *Cédula de Identidad* (with its own number) cardholders are issued two numbers, the *Rol Único Tributario* (RUT), an identifier for tax purposes, and the *Rol Único Nacional* (RUN), their number in the national civil register. The RUT is used alongside the card to complete interactions with the Tax Agency and the RUN with public and private sector organisations including the following:

- Buy or sell property and cars
- Obtain a Chilean driving licence
- Open bank accounts
- Collect loyalty points in shops

**Figure 3.1. Chile in comparison to the enrolment and population registries of the benchmarked countries in this study**



*Source:* Based on information provided by Austria, Canada, Denmark, Estonia, India, Italy, Korea, New Zealand, Norway, Portugal, Spain, United Kingdom and Uruguay in response to the OECD survey Benchmarking Digital Identity Solutions (Unpublished)

The use of the national civil register means that Chile's future development of DI has an important foundation. This existing identity, validated by the public sector, affords Chile the opportunity to focus less on working with the private sector to establish and identity and more on working with the private sector to establish interoperability and user experience standards that simplify the identity landscape for citizens in terms of how they access services. Such an approach could build on the experiences of the following countries:

- Sector specific DI (model 1) as found in **Uruguay**
- Sector specific DI (model 2) with a reusable public sector provided identity for private sector services as found in **Spain, New Zealand and Portugal**
- The public sector DI (model 5) as the basis for accessing both public and private sector services as found in **India and Italy**.
- A shared DI (model 6) where the Chilean government would work with the private sector to develop a single, shared DI built on the national civil register and able to access both public and private sector services as found in **Austria, Denmark and the United Kingdom**
- An interoperable DI (model 7) where both private sector DI and public sector DI are built according to standards that allow for public sector and private sector

services to be used by either public or privately provided DI as found in **Canada, Korea, and Estonia**

### *Characteristics of Chile's National ID card*

The Chilean National ID card contains several of the characteristics laid out in Chapter 2 (see section Dimension 1.1: National identity infrastructure. Characteristics of National ID cards). Chile uses polycarbonate as its material and follows the global standard for identity cards of ISO/IEC 7810:2003 ID-1. The *Cédula de Identidad* features the following elements:

- **Identification of the country**
- **Citizen photo**
- **Biographic information including the name, birthdate, nationality, and biological sex of the holder**
- **Validity information such as the date of issue, or of expiry and the document number**
- **A reproduction of the card holder's signature**
- **A representation of the data contained on the card encoded in a machine readable format, known as the Machine Readable Zone or MRZ. This is augmented by the use of a QR code to verify the validity of the document.**
- **Physical card security features including holograms and holographic symbols, embossing, variable colour printing, fluorescent elements, and elements visible only under ultraviolet light.**

The *Cédula de Identidad* contains a microchip format smart card which holds biometric data in a photograph and a right thumbprint of the holder.

This all contributes to the card having three layers of security:

- Level 1: security elements that can be seen by observing the card
- Level 2: elements that can only be seen using tools such as UV lamps and magnifying glasses
- Level 3: elements that are only visible to experts using microscopes or special reading devices.

Several of the countries considered for this study have identity cards which contain a chip. **Estonia** and **Portugal** have chips that require contact to be read, **Italy** has a contactless chip and **Spain** and **Uruguay** have a dual interface allowing for both contact, and contactless, reading of the card.

### *Enrolment for Chile's National ID card*

Anyone aged over 18 and resident in Chile is required to have a *Cédula de Identidad* identity card, but it is possible to obtain one at a younger age if so desired. This mandatory requirement is matched by the experiences of **Austria, Estonia, India, Korea, Portugal, Spain, and Uruguay**. Citizens have to pay a fee of 3 280 Chilean Pesos (EUR 4.27) for their card which is cheaper than any of the countries surveyed for this study.

To obtain the document for the first time citizens must attend an office of SRCeI and complete the process in person. This is to ensure the security and authenticity of an application for the identity card by the provision of physical documentation and the capture of biometric data. Appointments for this process can be made by telephone or online.

Should a citizen need to renew, or replace, their card whilst they are abroad then this is possible using the number of the *Cédula de Identidad* or the RUN.

This contrasts with the experience of **Austria, Spain, Estonia, Italy, India** and **Uruguay** who all handle part of this application process online, **Portugal** which has developed an entirely digital approach. Nevertheless, these countries have also maintained an analogue enrolment process, recognising that services should be *digital by design* rather than digital by default to ensure access for all.

### *DI policy*

Some parts of the Chilean public sector have existing DI approaches for enabling their services to be accessed online but one of the obstacles to the transformation of the citizen experience has been processes which usually require the use of a physical ID card as a starting point. As a result, the majority of services in Chile must still be completed face to face through the *ChileAtiende* network or the physical locations of other government service providers.

The launch of *ClaveÚnica* in 2012 was a direct response to this challenge and reflects the current model for DI in Chile. The administration of *ClaveÚnica* involves both SRCeI and DGD and uses the identity infrastructure discussed above to provide citizens with a single DI based on a username and password that complements the physical ID card which citizens already possess. However, it is not the only DI approach within the Chilean government with there being other competing approaches provided by different parts of the Chilean public sector.

Nevertheless, President Piñera gave *ClaveÚnica* a clear mandate in his Presidential Instructive on Digital Transformation (Instructivo presidencial sobre Transformación Digital) (Government of Chile, 2019<sup>[1]</sup>):

*“...los servicios públicos en sus plataformas digitales de trámites o servicios sólo podrán utilizar la ClaveUnica como instrumento de identificación digital, para las personas naturales, reemplazando cualquier otro sistema de autenticación propio del respectivo órgano de la Administración.”*

*“...public services in their digital platforms of procedures or services may only use the ClaveUnica as an instrument of digital identification, for natural persons, replacing any other authentication system proper to the respective body of the Administration.”*

More recently, the role of *ClaveÚnica* has been restated through the Presidential Instructions on Digital Transformation of January 24th 2019 (Presidente de la República de Chile, 2019<sup>[2]</sup>). This is in addition to DI being one of the six lines of action identified in the Government’s Digital Transformation Strategy (MINSEGPRES and DGD, 2019<sup>[3]</sup>). The ongoing need to redesign services has shown that challenges have existed around adoption, however the Presidential Instructions created a roadmap for more than 300 central government institutions to progressively incorporate *ClaveÚnica* as its only authentication mechanism for citizens by December 31, 2020. This will not be a minor undertaking as there are 1307 procedures of 3,537 that need an authentication mechanism

(37%). Of the 1307, only 477 use Unique password (37%) and the remaining 830 procedures use another authentication mechanism (63%). (see more detail in the section later in this chapter on Chile's DI platform).

As with the majority of countries considered in this study Chile has made DI, and specifically *ClaveÚnica*, a fundamental part of their Government's Digital Transformation Strategy so that the revitalised model for identity can:

1. Improve user experience and allow for greater personalisation of services through *Mi ChileAtiende*
2. Provide digital access to government services
3. Increase security
4. Transform the digital economy (including private sector services)
5. Reduce the cost of doing business in the country

Whilst it is important to establish a mandate for governments to adopt DI, it is equally important to ensure that citizens have confidence in the security and usability of the DI model. One important factor in achieving this is the role of national digital security strategies to ensure the DI model is secure for government and its users. Another important aspect is the ways in which citizens are in control of their data and it is therefore encouraging to see the intent for the future development of *ClaveÚnica* to provide digital tools that allow them to grant, and revoke, permissions for its use, reflecting the experience of **Austria** amongst others.

Chile does not currently have plans to expand the use of their DI to those who live outside the country in the way that **Estonia** has done through its e-Residency project.

### *DI governance*

As underlined previously in this study, the leadership and development of politics, policies and processes governing DI is critical to its success. Although there is a Presidential mandate for *ClaveÚnica* it is not yet the single mechanism for authentication and validation in Chile. Because identity is such a critical enabler to the digital transformation of governments it is often the case that multiple institutions will have taken their own approaches to implementing DI. This is particularly found in the experience of the organisations responsible for taxation and Chile is no different with the Chilean tax office (SII) (*Servicio de Impuestos Internos*) has an established model for identity and provision of online services. Alongside any organisation specific DI models there are two actors involved in leading the implementation and development of approaches to identity in Chile:

- The DGD within MINSEGPRES is responsible for the country's broader digital transformation including the Government's Digital Transformation Strategy (MINSEGPRES and DGD, 2019<sub>[3]</sub>). In supporting the digital transformation of the Chilean state DGD provides guidance, consultancy and technical support to the teams delivering on the future vision for services in Chile
- SRCeI administers both the existing identity infrastructure and previous efforts for the digital transformation of identity in Chile, including the original implementation of *ClaveÚnica*. SRCeI has previously commissioned the Universidad de Chile to consider how it might transform the experience of identity in Chile.

Both actors work together to operationally implement DI in Chile and develop ClaveÚnica. SRCeI maintains the process of validating the identity of citizens and their enrolment into the platform, and DGD is responsible for delivering the authentication and interoperability service of ClaveÚnica, managing the technological infrastructure that allows citizens to identify themselves and interact electronically.

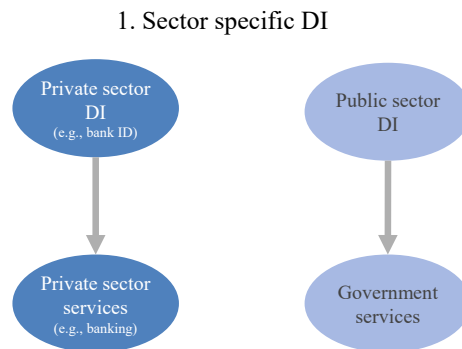
Chile is currently discussing whether there should be an additional actor created to oversee the governance and provision of DI in terms of protecting personal data. Whilst Law No. 19,628 effectively regulates data protection there is not currently a third party acting as a decentralised technical body for the supervision, surveillance and protection of the rights enshrined in the Law or with the authority to regulate, supervise, prosecute and, ultimately, punish breaches of it. As Chile explores how to create this capacity it is nevertheless important for such an entity to be independent of government whilst also ensuring anyone implementing a DI solution recognise and reflect on broader questions of data protection.

It could be attractive to locate all those working on questions of identity management within the same organisation to ensure that there is a focal point for both policy and delivery around identity whether analogue or digital. The countries in this study have approached the political leadership for identity in different ways with **Italy, Portugal, the United Kingdom and Uruguay** choosing to locate it closely with the head of government, **Estonia, Korea, New Zealand and Spain** maintaining ownership by the ministries responsible for Internal Affairs or the Interior Ministry, **Canada and Denmark** the Finance Ministry, and **Austria, India and Norway** with those responsible for digitalisation. Common to each of these approaches is a recognition that identity policy requires the authority and mandate of a central authority with cross-cutting responsibility for transforming the public sector. Furthermore, each of the approaches places identity management in the same organisation as digital government.

The current separation in Chile is not ideal, especially as DGD does not currently play the leading role in the design and implementation of this key enabler. Nevertheless, the Presidential Instruction on Digital Transformation on January 24<sup>th</sup> 2019 identified that DGD would have the lead responsibility for leading the implementation of DI for citizens executing the necessary coordination and delivery actions. This recognises the key role of the DGD in supporting the operationalisation and deployment of some of the key enablers for digital government in the country, but weakens its full ownership of the design and conceptualisation phase.

This is important because Chile currently reflects the sector specific DI approach shown in Figure 3.1). However, unlike the simplicity of that model which suggests a single private sector DI and a single public sector DI, ClaveÚnica is in fact only one of several authentication mechanisms within either government, or the private sector. This means that for the citizen there is a proliferation of approaches to identity that will need to be rationalised or consolidated to deliver on the promise of DI for Chile and to enable partnerships with the private sector that transform access to services.

**Figure 3.2. Chile's existing model of DI**



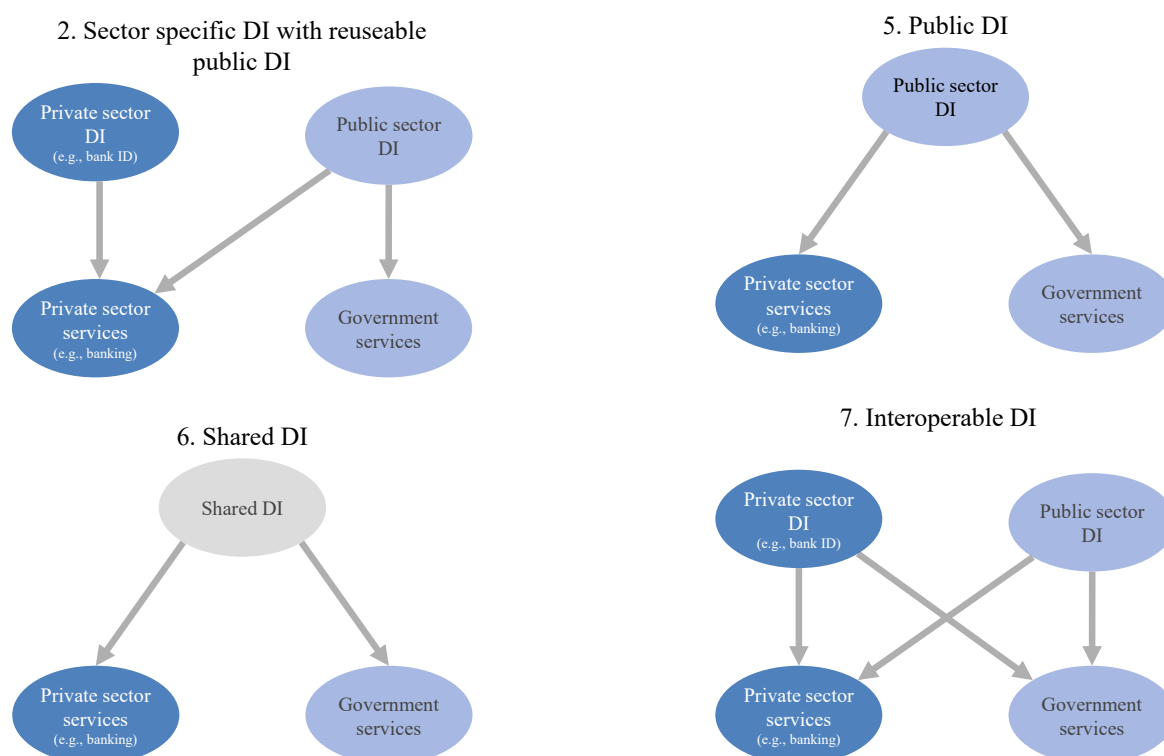
The majority of countries in this study have adopted models that allow for DI to be used across both public and private sector services and there are clear benefits from pursuing an approach to the design of the solution which favours interoperability and reuse across both domains. The existing analogue identity model in Chile allows for the use of the *Cédula de Identidad* in accessing private sector services and the future vision for *ClaveÚnica* recognises the same potential. Forging partnerships with the private sector to ensure that the way in which the Chilean government approaches identity has mutual benefits in transforming services and supporting adoption is clearly to be preferred. Such an approach will require strong governance and effective delivery to realise its potential.

DI models that serve the public sector only have more straightforward governance arrangements due to avoiding operability with external private systems and regulating the user experience of those private solutions. However, models which do not promote cooperation between the sectors are consequently limited in their levels of reuse and adoption. Therefore, approaches which reuse existing (public or private) DI, develop shared models, or consider public and private sector applications are preferable.

With the strength of SRCeI, the Chilean government's commitment to an interoperable *ClaveÚnica* and the familiarity of the Chilean public with the *Cédula de Identidad* models 2, 5, 6 and 7 which focus on the reuse of a public or shared DI are best suited to further exploration in Chile.



Figure 3.3. Potential DI models for Chile



## Chile's technical DI solution

### *DI platform*

The platform for DI in Chile is *ClaveÚnica*. The current iteration of *ClaveÚnica* offers a straightforward web authentication model using a user identifier and password for browser based services. It is built on the underlying identity mechanisms of the *Cédula de Identidad* provisioned by SRCeI. *ClaveÚnica* enabled services are also available through kiosks located within *ChileAtiende* locations.

Enrolment for *ClaveÚnica* requires any citizen over the age of 14 to attend an office of SRCeI with a valid *Cédula de Identidad* and request a *ClaveÚnica* activation code that will be emailed to them. Once that activation code has been received then they visit [claveunica.gob.cl](http://claveunica.gob.cl) and use that with their RUN to create a unique *ClaveÚnica* password.

In this situation the verified identity on which *ClaveÚnica* relies and the product itself is provided by SRCeI. The DGD is responsible for identity policy, adoption of *ClaveÚnica* and the broader cross-government thinking about the opportunities and value of DI.

Although *ClaveÚnica* is currently only offering browser based authentication, the future ambition is intended to allow for (as referenced earlier):

1. **Data authentication:** the mechanism by which citizens will be identified to access state services and other private organisations
2. **Data wallet:** A store of personal data for citizens which will allow interoperation with institutions on the basis of permissions which a citizen grants on their information

3. **Advanced electronic signature:** Users of ClaveÚnica will be able to sign electronic documents issued by public bodies
4. **Citizen mailbox:** A means by which the state will notify citizens of important information and progress on their interactions with the state
5. **Web portal eID:** a website where citizens can manage access to their data, grant and revoke permissions and update their personal data

The future technical approach for ClaveÚnica is to be built on OpenID Connect and use the OAuth 2.0 framework. This means that ClaveÚnica is highly interoperable and consists of a lightweight infrastructure that does not require extensive funding to support and maintain. Such an approach favours the adoption of ClaveÚnica in both the public and private sectors.

In providing only simple authentication ClaveÚnica does not currently offer the means of providing additional attributes which expand the scope of how the DI is used. This contrasts with the experience of **Austria, Italy, and Portugal** where their DI provides access to attributes including tax information, address, birthdate, and professional information. However, the vision for the ClaveÚnica platform is that this simple model will evolve to support the transformation of services in ways that move beyond simple authentication and basic digitisation of analogue processes.

### *Smartcards*

The *Cédula de Identidad* is an important part of the DI solution in Chile. It is a smartcard and holds biometric data in the form of a right thumbprint of the holder and a photograph. In this respect it provides additional layers of security when accessing services in a face to face setting. However, it is not currently being used to offer any augmented functionality in conjunction with ClaveÚnica.

In the case of **Portugal, Spain and Uruguay** this information allows for them to implement a Match on Card approach to two factor authentication and for the verification that the person with the card is who they claim to be. In **Austria, Estonia, Portugal, and Spain**, their implementation of a smartcard model provides the basis for identity amongst particular professions where authenticated digital signatures are part of their daily lives.

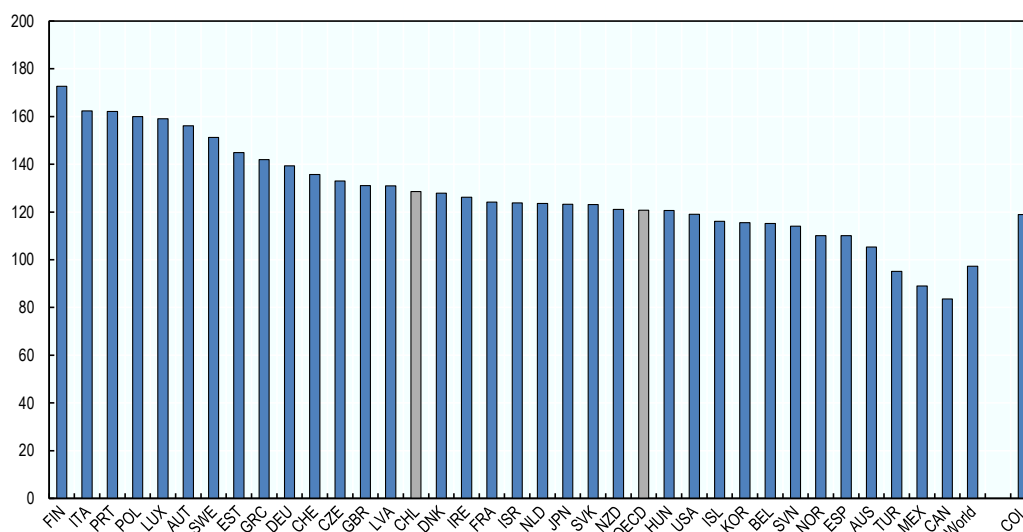
Nevertheless, smartcard approaches require the holder to have access to physical hardware and be comfortable with the use of the card in this way. It is not as well suited to those who might only be using this enhanced functionality on an infrequent basis. Furthermore, smartcard technology brings with it greater costs than some of the other factors being considered. As well as the overhead of obtaining physical infrastructure to support their use, the item cost of a card is usually borne by a citizen. **Austria, Estonia, Portugal, Italy, Uruguay, and Spain** all charge for these cards at an average of EUR 24 for an adult, which is significantly more than the current EUR 4.27 charged to Chileans for their *Cédula de Identidad*.

Therefore several countries, including **Austria**, have recognised that smartcards may not be the most effective method of mass adoption and have favoured mobile approaches instead. In doing this the DI approach can maintain security, evolve to reflect new technological possibilities and avoid the need for replacing the physical identity cards already held by the population.

## Mobile

ClaveÚnica does not currently require access to a mobile device, it is an authentication mechanism that works regardless of the device being used. This means not only through web browsers on computers and mobile devices but through kiosks located at *ChileAtiende* too. With figures for smartphone ownership and mobile internet access in Chile higher than the OECD average this could be an important enabler of DI for the country.

**Figure 3.4. Cellular mobile penetration, subscriptions per 100 inhabitants (2015)**



*Note:* The statistical data for Israel are supplied by and under the responsibility of the relevant Israeli authorities. The use of such data by the OECD is without prejudice to the status of the Golan Heights, East Jerusalem and Israeli settlements in the West Bank under the terms of international law.

*Source:* World cellular mobile subscriptions (OECD and ITU, 2017<sup>[4]</sup>)

From a heightened security point of view, mobile devices have been favoured as a mechanism for providing two-factor authentication in several of the countries included in this study. For Chile, the implementation of a second factor authentication approach using the creation of a One Time Pass (OTP) either through the receipt of SMS or the use of an authentication app on a mobile would be an important addition.

Furthermore, mobile approaches can simplify the application of more advanced security functionality like digital signatures. In Chile, Article 3 of Law 19,799 creates a functional equivalence between an electronic signature and a handwritten signature and mobile offers an attractive opportunity to enhance its utility in any context without the requirement for additional hardware. This is attractive both to infrequent users of the identity, and the providers of services themselves.

Moreover, with the future intent for ClaveÚnica to provide citizens with a data wallet, digital signature functionality and tools for the management of access to data there are obvious benefits to pursuing a mobile first approach.

## Biometric and emerging DI

The *Cédula de Identidad* contains biometric data in the photograph of the holder and the right thumbprint. Nevertheless, ClaveÚnica does not currently use this information to

support the delivery of services. Furthermore, the use of the biometric data held within the *Cédula de Identidad* introduces additional costs to the management of DI in Chile that may not represent good return on investment. As has been seen in the studied countries, the role of biometric data can provide opportunities to use biometric markers in providing higher levels of identity verification and a more coordinated experience of government across digital and analogue services. It is however not a priority in securing broad adoption for either users or providers of services.

The important foundations for identity provided by the *Cédula de Identidad* and SRCeI as well as the intended architecture for *ClaveÚnica* favouring interoperability mean that Chile is well positioned to prioritise ‘Bring Your Own Identity’, especially outside the public sector. The models in Figure 3.3 suggested for consideration by Chile all recognise the opportunities for an identity to provide sufficient trustworthiness to be adopted across the day to day experience of the public as an enhancement to email or social media credentials. The experience of **Portugal** and **New Zealand** amongst others in seeing their DI reused by telecoms, media and banking is particularly relevant to demonstrating the value of interoperable DI in transforming digital services and replacing the need for face to face service interaction.

## Policy levers and adoption

### *Legal and regulatory framework*

Chile’s Government Digital Transformation Strategy identifies DI as one of six strategically important lines of action to support the digital transformation of the Chilean state (MINSEGPRES and DGD, 2019<sup>[3]</sup>). This follows from President Sebastián Piñera’s first address of June 20th 2018 and the Presidential Instruction on Digital Transformation on January 24th 2019, identifying DI as one of four strategically important lines of action on its state modernization plan (Presidente de la República de Chile, 2019<sup>[2]</sup>). There is not only a clear statement of political intent in recognising *ClaveÚnica* as the preferred model for DI in Chile but a comprehensive mandate which requires teams within government to recognise it as such.

Whilst adoption is therefore mandated for service providers in government there is no legal requirement for citizens to be in possession of a DI. This contrasts with the legal requirement for residents over the age of 18 to be in possession of a *Cédula de Identidad*. This is common in those countries like Chile which have a national identity register and a physical identity card but Chile may wish to extend that requirement to the possession of a DI as is the case in **Denmark, Estonia, Korea, and Portugal**.

Law No. 19,799 first implemented in 2002 provides the legal basis for the use of electronic signatures in Chile. In Article 3 it identifies the functional equivalence between the act of signing something by electronic signature and a handwritten signature on paper.

Chile is developing data protection legislation to reflect the OECD’s Recommendation on the Protection of Privacy and Transborder flows of Personal Data (OECD, 2013<sup>[5]</sup>). Law No. 19,628 covers several important areas for underpinning the successful implementation of DI in Chile. They include the principles of:

- Legality in the processing of data (the use of personal data only with the consent of the holder or Legal provision)
- Purpose (use of data only for the purposes explicitly indicated)

- Proportionality (use of data limited to the purpose explicitly indicated)
- Quality
- Responsibility
- Security, and
- Information (provision of access to policies on data processing)

The existence of this law makes provision for some of the ambitions for interoperability contained within the Government's Digital Transformation Strategy and an imagined future where the country is able to work in a paperless fashion (MINSEGPRES and DGD, 2019<sup>[3]</sup>). The development of *ClaveÚnica* on the basis of open standards reflects a similar opportunity to champion interoperability. In both these cases the Technical Interoperability Standard in the State of Chile is an important document for supporting the implementation of DI and transformed government services.

One way in which the governments of **Austria**, **Canada**, **New Zealand** and **Portugal** have chosen to enhance their legislative framework in support of interoperability, data protection and DI is to prevent different government agencies from using identical identifiers for the same person. This approach means that any information being stored about an individual by one organisation is not easily joined to information held elsewhere if it is accessed by nefarious actors. The example of Austria's *SourcePIN* discussed earlier ensures that only the information which is necessary for a service to meet a need is ever stored.

A further important legal development related to the adoption of the 'once only principle' is found in several of the surveyed countries including **Denmark** and **Portugal**. The Presidential Instruction on Digital Transformation on January 24th 2019 considers the "Cero Filas" (Zero Rows) policy that mandates government departments not to require citizen documentation that is already in the State's possession, taking the necessary steps to interoperate and access the required information (Presidente de la República de Chile, 2019<sup>[2]</sup>).

Latin American and Caribbean countries have strengthened their cooperation on digital government, especially through the e-Government Network of Latin America and Caribbean (*Red de Gobierno Electrónico de América Latina y El Caribe*, Red GEALC) in recent years and are initiating conversations about developing a regional equivalent to the eIDAS regulation seen in the European Union, initially in the context of mutual recognition of digital signatures. Chile is developing a standards based approach to *ClaveÚnica* that could support cross-border identity but there is no regulatory provision for such an approach. Nevertheless Chile's recognition of Argentina's digital driving licence demonstrates the potential for enabling such cross-border services. Achieving regionally interoperable DI would not be a quick undertaking but one which may prove beneficial.

A final area of the legal and regulatory framework which is not currently in place in Chile relates to the interaction between the public and private sectors. The nature of this relationship in terms of the model for identity underpinning *ClaveÚnica* is still to be confirmed, but as Chile works through its understanding and implementation of the provision of identity, the use of that identity and the reuse of any data associated with that identity this legal and regulatory framework will need to be developed. The experience of the **United Kingdom** in managing the federated nature of its identity provision may be instructive. By developing several Good Practice Guides the UK set out its expectations for providers of identity in a way that didn't have legal weight but which established the

criteria by which their involvement would be approved or rejected (UK Cabinet Office, UK Government Digital Service and UK National Cyber Security Centre, 2018<sup>[6]</sup>).

### *Funding and Enforcement*

The commitment in President Piñera's address of June 20<sup>th</sup> 2018 and the Presidential Instruction on Digital Transformation on January 24<sup>th</sup> 2019, plus the ongoing work of DGD and SRCeI on implementing the expansion of ClaveÚnica demonstrate the commitment of funding for this work through the current political cycle (Presidente de la República de Chile, 2019<sup>[2]</sup>). This sits alongside the ongoing funding for SRCeI and its contribution to the country's national identity infrastructure. Through the Presidential Instruction on Digital Transformation on January 24<sup>th</sup> 2019, four axes were established for achieving State modernization, of which one is the implementation of DI for citizens, placing the responsibility on DGD to lead the process and execute the necessary coordination and delivery actions.

One way in which Chile is mitigating this risk is through a standardised model for producing business cases across the public sector. All government technology projects planned for the 2018/2019 period were presented using a common format and going through a review and technical approval process. This review and approval process requires thought to be given to role of DI and the use of ClaveÚnica reflecting the experiences of **Denmark, Portugal** and the **United Kingdom**.

Whilst the political imperative has been made clear and DI embedded into the funding approval process there is less detail on the delivery approach and associated support for helping ClaveÚnica achieve its ambitions and the Chilean public sector maximise its benefits. The reorganisation of DGD into four core services includes a focus on a function to facilitate the development and support of shared platforms following the Government as a Platform model. This additional capacity is intended to provide on the ground support and consultancy. The success of these efforts will be seen in the level of adoption they achieve. Whilst ClaveÚnica has received high level endorsement and a mandate for enforcing adoption there remains a need for all those, whether within DGD or SRCeI, involved in the provision of identity services to reflect the same focus of responding to needs as any public facing activities. Therefore, ClaveÚnica should be approached with an approach that starts from the premise of meeting needs well.

Alongside the technical capability to deliver ClaveÚnica as a secure and reliable platform, effort needs to be invested in simplifying its initial adoption so that a minimum of effort is required to implement a solution or persuade a team to adopt. Critical to this success is allowing delivery teams to make use of a shared resource as quickly and easily as possible. These efforts would be supported by thought being given to the role of engagement and account management for 'customers' elsewhere in government. Such roles will complement product level user research by helping DGD and SRCeI understand any barriers to adoption and help to augment the way in which ClaveÚnica describes its value proposition, surfaces its technical documentation and frames its associated benefits.

Finally, from an internal perspective, Chile is still developing central resources that provide guidance to shape delivery and setting standards with which to assess the quality of that delivery. It will be important for these service delivery standards and guidelines to consider the role of identity and the design of the services which rely on it.

In terms of encouraging adoption of ClaveÚnica amongst the public there is no explicit intent to seek funding for marketing campaigns. Instead, the team at DGD and SRCeI have

expressed their commitment to developing adoption of *ClaveÚnica* in line with the needs of citizens rather than growing the number of people holding a DI but with limited opportunities to use it. The *ChileAtiende* and SRCeI networks represent an important element of how Chile is supporting its citizens to make use of *ClaveÚnica* and to develop the digital literacy of its citizens.

### *Government services*

Transformation of the user experience of government is one of the biggest motivations for implementing an effective model of DI. By being able to rely on a secure and effective DI, citizens are able to meet their needs without having to be physically present. The highest priorities for implementing DI were taxation, education and health.

In Chile, 49% of the nation's 3 537 procedures can be carried out online. Of those, there are 1307 that need an authentication mechanism (37%). Of the 1307, only 477 use *ClaveÚnica* (37%) and the remaining 830 procedures use another authentication mechanism (63%). DI is an important priority for enabling the transformation of the citizen experience. In particular the policies of “*Cero Filas*” (Zero Rows) and “*Cero Papel*” (Zero Paper) aim to turn Chile into a truly paperless state with institutions committed to digitising services and using *ClaveÚnica* to support it. In some cases the country is mandating the use of *ClaveÚnica* to continue to receive benefits, with one case producing increased adoption by 1.5m people in one month.

A second example is *Empresa en un dia*, a programme making it possible to create a business in a single day. *ClaveÚnica* adds initial value to this service but in working with the programme it is expanding the offer of *ClaveÚnica* to include electronic signatures and establish a business focused approach that allows citizens to link their business identity with their personal identity. By meeting several common needs, *ClaveÚnica* reflects aspects of Government as a Platform thinking that will accelerate the transformation of other services that would otherwise have to develop their own approach.

Whilst the primary focus of DI is initially central government services, more than half of the surveyed countries anticipate the adoption of DI within local governments and other channels, as highlighted in the previous chapter. This is an important area for Chile to consider given the existing landscape of service provision in Chile makes use of the *ChileAtiende* network as well as physical locations for several other public bodies. Currently the delivery of online or telephone based services is limited by the limited application of DI in Chile and this is a priority for Chile in developing its strategy for service design and delivery.

Chile is following a standards based approach which offers the potential for Chile and its regional partners to emulate the experience of eIDAS amongst the European Union member states in establishing a common, interoperable, approach to identity. The recent development of Argentina's digital driving licence, which is recognised in Chile is an important demonstration of the potential for enabling cross-border services.

An area that was absent from conversations about the enabling role of DI in Chile was its impact on those working within government. More than half of the countries discussed earlier (**Denmark, Estonia, India, Korea, Norway, Portugal, Spain and Uruguay**) have prioritised the needs of public servants in their approach to DI. The internal benefits of being able to validate the identity of someone and the ease with which such a solution can be deployed have benefits that should not be overlooked.

### *Private sector services*

Approaches to DI that encourage its use by both government and private sector services increase both visibility and familiarity. This amplifies the relevance of a DI mechanism as citizens use it more regularly than if they were solely limited to its application for public sector services. The reusability and interoperability of a given DI for accessing both government and private sector services adds value to citizens who don't need to manage multiple credentials or constantly create new accounts to prove who they are.

ClaveÚnica currently enables in excess of 5m Chileans to access services in the public sector but the ambition is for it to expand to incorporate private sector services, including the banking sector. One of the most important developments in that respect is the addition of a second factor of authentication to complement the existing ClaveÚnica mechanism.

With a technical solution built on OpenID Connect and using the OAuth framework the ClaveÚnica solution is highly interoperable and consists of a lightweight infrastructure that does not require extensive funding to support and maintain.

The Chilean private sector is already familiar with reusing the identity infrastructure provided by the *Cédula de Identidad* and the RUT and RUN identifiers. This provides Chile, and ClaveÚnica with an important starting point from which to consider its wider application.

As discussed in Figure 3.3 there are four models, which would lend themselves to the ambition and context in Chile for building on the country's existing identity infrastructure to enable access to private sector services. The experiences of **Austria, Denmark, Estonia, India, Italy, New Zealand, Norway, Spain**, and the **United Kingdom** in recognising the potential for DI to enable Business to Consumer (B2C) services provided by the private sector.

### *Enablers and constraints*

The benchmarking study identified six areas – business model, hardware infrastructure, awareness, enrolment, user experience and digital literacy - that have the potential to be seen as an enabler, or a constraint for DI in a country.

For Chile, the **business model** associated with DI is yet to be formally decided. The country has an existing basis for verified identity in the *Cédula de Identidad* that is an enabler to the integrity of ClaveÚnica. The technology underpinning ClaveÚnica is designed to enable interoperability with private sector services. Chile has the opportunity to decide how it shapes the business model for ClaveÚnica and its enhanced functionality as it works with public sector and private sector service providers and encourages adoption within the country.

The *Cédula de Identidad* is a smartcard that requires **hardware infrastructure** to unlock its most secure features. However, none of that functionality is exploited by ClaveÚnica or the model for DI in Chile and therefore hardware infrastructure is neither an enabler nor a constraint. The relatively high incidence of mobile phone penetration in Chile underpins future ambitions for ClaveÚnica to focus on the opportunities available through web and mobile platforms.

The existing model of identity in Chile means that there is high **awareness** of processes involving the *Cédula de Identidad*. This provides a good enabler for adoption of ClaveÚnica. Nevertheless, awareness and adoption of ClaveÚnica will reflect its availability in terms of accessing services that people need. The potential in this area is



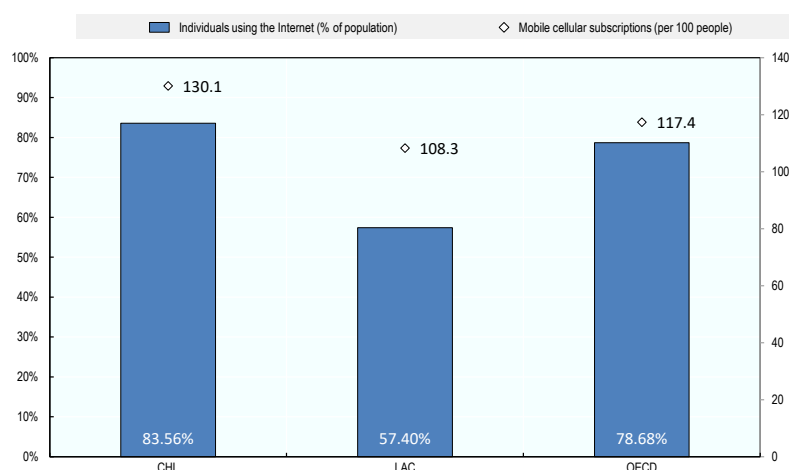
seen by the example of a service which switched to *ClaveÚnica* and increased adoption by 1.5m people in one month. The most significant barrier to its usage is the limitations on the number of services which are *ClaveÚnica* enabled but, as discussed elsewhere, the Presidential mandate to see more services switch to using it should encourage adoption of the current model of *ClaveÚnica* and provide a boost to later adoption of the planned enhanced functionality.

As with awareness, the **enrolment** experience for *ClaveÚnica* benefits from being built on top of the *Cédula de Identidad* and this should be seen as an enabler. However, the process by which someone obtains a *ClaveÚnica* is still reliant on a face to face interaction.

Nevertheless, the overall **user experience** of *ClaveÚnica* is effective, acting as an enabler for those who wish to use it to access services online or at a *ChileAtiende* kiosk. As Chile progresses with the channel shift to digital services it is critical that the necessary support is made available for those who might not be comfort using digital channels. The issue of digital inclusion is therefore critical to the adoption of DI.

Whilst the ease of using *ClaveÚnica* online is relatively straightforward the broader Chile performs reasonably well in terms of access to the internet standing above the LAC and OECD averages in terms of share of the population using the internet and mobile subscriptions per 100 people (Figure 3.5). Given the diverse and complex geography of the country this is an impressive achievement. Nevertheless, the question of **digital literacy and access** is an important consideration in the adoption of DI in Chile with there being a gap in terms of the population that has access to the internet and the number of individuals who choose to transact with the public sector digitally. Chile's National Survey of Socioeconomic Characterisation (*Encuesta de Caracterización Socioeconómica Nacional*, CASEN) found that 30.1% of the population used the internet to complete a government procedure over the last year (MIDESO, 2017<sup>[7]</sup>).

**Figure 3.5. Proportion of internet users and mobile subscriptions, 2016**



Source: World Development Indicators, <https://datacatalog.worldbank.org/dataset/world-development-indicators> (World Bank, 2016<sup>[8]</sup>)

## Transparency and monitoring

### *Citizen control of their data*

Neither *ClaveÚnica* nor the *Cédula de Identidad* currently offer a means by which citizens can control their data and see the detail of how their data are being accessed and/or used. However, the future ambition for DI in Chile places this at its heart. With Chile anticipating that *ClaveÚnica* will provide a data wallet for citizens and a website where permission can be granted and revoked there is particular relevance in the experience of **Spain**. *Carpeta Ciudadana* provides a means of seeing an audit trail which includes not just their own login activity but the detail of how organisations have used their data.

### *Performance data*

Certain performance indicators are published on the homepage for *ClaveÚnica*. These reflect the number of active users, institutions, processes and daily authentications. Although it is important to recognise the importance of the availability of this information, it is not as extensive as some of the other dashboards featured in this study.

**Figure 3.6. Certain performance metrics on the *ClaveÚnica* homepage**

(<https://claveunica.gob.cl>)



Source: ClaveÚnica website (Chilean government, 2019[17])

Furthermore, it is important for Chile to consider whether these measures are providing the necessary level of information to respond with any changes that might be required to improve the user experience of *ClaveÚnica* and to address any barriers to adoption. Moreover, as the vision for the future *ClaveÚnica* is implemented it will be important to track its performance according to relevant and insightful KPIs.

The use of the RUN and reliance on the existing *Cédula de Identidad* affords the Chilean government an opportunity of establishing a view of services accessed by citizens both online and in person across government. This provides an important source of data for broader service transformation, but must be treated with caution. As discussed previously, **Austria, Canada, New Zealand** and **Portugal** have enacted laws that require the disaggregation of data about individuals.

### *Impact assessment*

The majority of countries surveyed as part of this study did not conduct extensive analysis of the impact of their DI approach. There is little evidence that Chile currently carries out a sophisticated approach to measuring the impact of its DI and has not yet made this part of the plans for the future of *ClaveÚnica*.

Nevertheless, the Study for the Formulation of a Modernization Project of the Civil Registry and ID (Universidad de Chile, 2017<sup>[9]</sup>) identified several areas in which impact and performance could be measured. These include:

- The usage of DI both in terms of raw usage and implementation
- The success of DI reuse between the public and private sectors and interoperability of data that has enabled a reduction in its requesting, processing and storing
- The impact of DI on the internal operations of the SRCeI and the transition from paper to digital records
- The transformation of analogue processes experienced by the public and the opportunities for redesigning their experiences
- The tracking of skills development amongst staff and the public

These highlight the value in understanding performance in order to measure impact, both on citizens in terms of the benefits to their daily lives, but also to the state itself in terms of the transformation of the experience and any efficiency.

## References

- Chilean Government (2019), ClaveÚnica, <https://claveunica.gob.cl/> (accessed on 3 April 2019).
- Chilean Government (2019), *Presidential Instructive on Digital Transformation*, <https://digital.gob.cl/instructivo/acerca-de> (accessed on 28 August 2019).
- MINSEGPRES and DGD (2019), *Estrategia Transformación Digital*, [https://digital.gob.cl/doc/estrategia\\_transformacion\\_digital\\_2019\\_v1.pdf](https://digital.gob.cl/doc/estrategia_transformacion_digital_2019_v1.pdf) (accessed on 10 July 2019).
- OECD (2013), *Recommendation of the Council concerning Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data*, OECD, Paris, <https://legalinstruments.oecd.org/en/instruments/OECD-LEGAL-0188>.
- OECD and ITU (2017), *World Telecommunication/ICT Indicators* (for cellular mobile subscriptions).
- Presidente de la República de Chile (2019), *Instructivo Presidencial en Transformación Digital*.
- UK Cabinet Office, UK Government Digital Service and UK National Cyber Security Centre (2018), *Identity proofing and authentication* - GOV.UK, <https://www.gov.uk/government/collections/identity-proofing-and-authentication>.
- Universidad de Chile (2017), *Estudio para la Formulación de un Proyecto de Modernización del Servicio de Registro Civil e Identificació.*
- World Bank (2016), *World Development Indicators* (WDI), <https://datacatalog.worldbank.org/dataset/world-development-indicators> (accessed on 3 April 2018).

## **ORGANISATION FOR ECONOMIC CO-OPERATION AND DEVELOPMENT**

The OECD is a unique forum where governments work together to address the economic, social and environmental challenges of globalisation. The OECD is also at the forefront of efforts to understand and to help governments respond to new developments and concerns, such as corporate governance, the information economy and the challenges of an ageing population. The Organisation provides a setting where governments can compare policy experiences, seek answers to common problems, identify good practice and work to co-ordinate domestic and international policies.

The OECD member countries are: Australia, Austria, Belgium, Canada, Chile, the Czech Republic, Denmark, Estonia, Finland, France, Germany, Greece, Hungary, Iceland, Ireland, Israel, Italy, Japan, Korea, Latvia, Lithuania, Luxembourg, Mexico, the Netherlands, New Zealand, Norway, Poland, Portugal, the Slovak Republic, Slovenia, Spain, Sweden, Switzerland, Turkey, the United Kingdom and the United States. The European Union takes part in the work of the OECD.

OECD Publishing disseminates widely the results of the Organisation's statistics gathering and research on economic, social and environmental issues, as well as the conventions, guidelines and standards agreed by its members.

# Digital Government in Chile – Digital Identity

In our interactions with the people we know we don't give any thought to the proof of their identity. When we meet someone for the first time we trust they are who they say they are. Sometimes an introduction is brokered by a mutual, trusted, acquaintance who knows both parties. However, in our transactional dealings with government there is a greater expectation – and need – to be able to prove who we are, where we live and what we can access. The provision of digital identity (DI) is critical to government ambitions for transforming the quality of public services.

This study discusses Chile's experience of DI alongside a comparison of 13 OECD countries, and aims to support the Government of Chile in developing and enhancing their approach to the development of DI as a piece of core digital government infrastructure and an enabler of seamless service delivery. The study uses a framework that covers the foundations for identity in terms of existing national identity infrastructure, policies and governance, the technical solutions that have been explored, the factors which impact adoption, and the ways in which DI can empower citizens through greater control of their data, transparency and measurement of impact.

This publication is a contribution to the OECD Going Digital project which aims to provide policymakers with the tools they need to help their economies and societies prosper in an increasingly digital and data-driven world.

For more information, visit [www.oecd.org/going-digital](http://www.oecd.org/going-digital)

#GoingDigital



Consult this publication on line at <https://doi.org/10.1787/9ecba35e-en>.

This work is published on the OECD iLibrary, which gathers all OECD books, periodicals and statistical databases. Visit [www.oecd-ilibrary.org](http://www.oecd-ilibrary.org) for more information.

