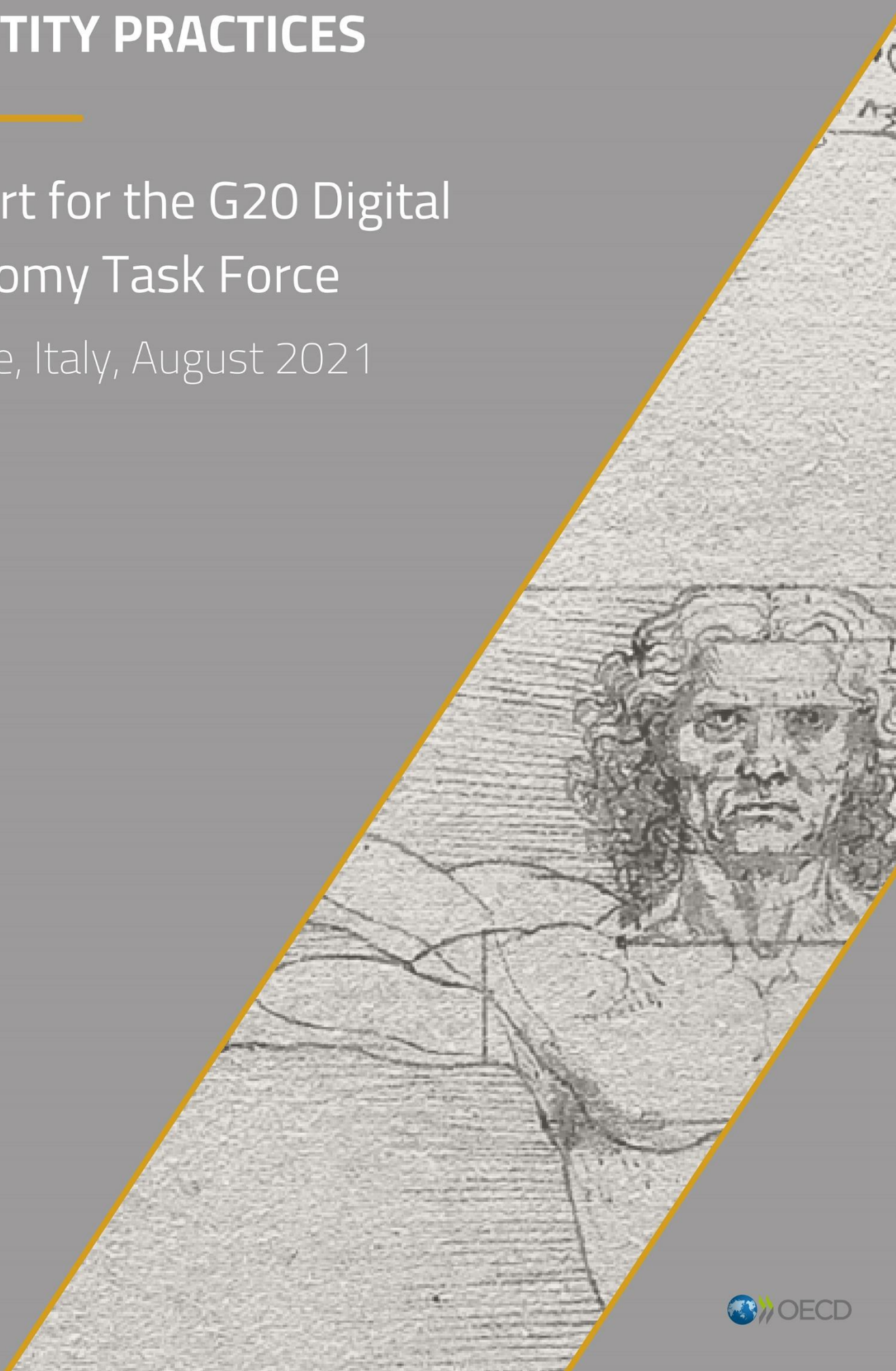
G20 COLLECTION OF DIGITAL IDENTITY PRACTICES

Report for the G20 Digital Economy Task Force

Trieste, Italy, August 2021



G20 ITALIA 2·0·2·1

OECD

This document was prepared by the Organisation for Economic Co-operation and Development (OECD) Directorate for Public Governance (GOV), to inform the discussions in the G20 Digital Economy Task Force at the request of the G20 Italian Presidency in 2021. The opinions expressed and arguments employed herein do not prejudge or necessarily represent the official views of the OECD or G20 members.

Foreword

The digital transformation of our economies has accelerated significantly during the COVID-19 pandemic. Use of digital services has rapidly expanded and governments have needed to ramp up the digitalisation of existing public services as well as introduce and provide many new digital services to fight the pandemic responding to the evolving needs of households and business, and to get the recovery underway.

This unprecedented level of innovation in the public sector is very encouraging. Optimising the use of digital technologies and data will not only increase the efficiency of the public sector, it will also transform the way governments design and deliver services, in a more user friendly way, tailored to the evolving needs of our communities. People expect digitally-mature governments to seize these opportunities and shape the digital transformation to ensure everyone has the opportunity to participate and benefit, while also appropriately managing the risks associated with digitalisation.

Under its 2021 G20 Presidency, Italy made digital governance one of its priorities to build on the momentum from the pandemic and engage resolute action for sustainable, comprehensive and coherent transformation of government in the digital age. With the support of the OECD, the G20 Digital Economy Task Force (DETF) advanced the global debate on how to address the digital transformation of our governments from three crucial perspectives: digital tools for public services and their continuity, digital identity and agile regulatory governance to harness innovation.

Furthering the work undertaken by the previous Presidencies of Argentina and Japan, with the G20 Digital Government Principles, and the G20 AI Principles, this renewed momentum around digital government in the G20 will pave the way for ambitious collective action and build on the key messages emerging from the evidence and analysis in these three reports:

1) The "**G20 Compendium on the use of digital tools for public service continuity**", with 120 practices collected across G20 members, indicates how governments can significantly transform themselves and make the best use of digital technologies, such as AI, and data to better serve societies and economies, learn from each other and accelerate the development of most successful use cases. Focusing on the quality, sustainability and trustworthiness of digital government services would be a natural way forward for the G20.

2) The "**G20 Collection of Digital Identity Practices**" highlights how digital identity is a core 21st century service for mature digital government and developing trusted citizen-to-Government relationships as it can grant people access the services they need, wherever and whenever they need them without any friction or impediment. Much remains to be done for portable digital identity solutions that can be trusted by all. This foundational stock-taking exercise, initiated by Italy is conceived as an initial stepping stone to improve access to all, with the long term objective of cross-county interoperability.

3) The "**G20 Survey on Agile Approaches to the Regulatory Governance of Innovation**" showcases ongoing efforts of G20 governments to revisit how they regulate in this fast-paced global innovation landscape. It also leveraged the OECD Recommendation on Agile Regulatory Governance to Harness Innovation as a tool for governments to fully benefit from the power of innovation while better managing their potential unintended consequences, through transparency, experimentation and shorter regulatory cycles.

To optimise the strength and the quality of the COVID-19 recovery, we need to facilitate the digital transformation of the public sector with forward looking future oriented governance structures. This crisis has forced all governments to rethink how they operate, regulate and interact with their citizens, and to accelerate deployment of digital public services and applications at a speed and scale unimaginable before the pandemic. Governments should sustain these transformational efforts in the long run. It will make them more agile, responsive, inclusive, innovative, trustworthy and better equipped to respond to future global threats. The newly established G20 Digital Economy Working Group is well placed to further these initiatives by sharing impactful and exemplary deployments and approaches. The government of Italy and the OECD stand ready to build on these foundations with future G20 Presidencies.

Mathias Cormann,

OECD Secretary-General

Vittorio Colao

Italian Minister for Technological Innovation and Digital transition

Table of contents

Tables

Figures

Boxes

Acknowledgements

This report was produced under the G20 Italian Presidency. It was prepared by the OECD Directorate for Public Governance, under the leadership of Elsa Pilichowski. It was produced by the OECD Open and Innovative Government Division, under the supervision of Barbara-Chiara Ubaldi, Acting Head of Division and Head of the Digital Government and Data Unit.

The report was written by Benjamin Welby and Cecilia Emilsson from the Digital Government and Data Unit. All sections benefitted from the strategic review of Barbara-Chiara Ubaldi and Charles Baubion, Advisor, Director's Office, OECD Public Governance Directorate. Colleagues from the OECD Science, Technology and Innovation Directorate reviewed and provided comments.

The paper relies on contributions detailing the digital identity experiences of Argentina, Australia, Brazil, the European Union, Germany, Indonesia, Italy, Russia, Saudi Arabia, Singapore, Spain, Turkey, and the United Kingdom. Information was also provided by Democratic Republic of Congo and Mexico where digital identity solutions are currently under development while in the United States of America, identities are generated at the local government level and used to create state government level identity credentials rather than there being a single federal solution. Information was not available for Canada, China, France, India, Japan, Korea and South Africa.

Executive summary

Under the 2021 Italian Presidency, the G20 recognised digital identity as a priority for achieving social and economic inclusion, forming part of its broader commitments to advancing digital government through the work of the G20 Digital Economy Task Force (DETF).

As enshrined in the Universal Declaration of Human Rights, all individuals have the right to be recognised as a person before the law. There is still much to do to address the need for and basic right of individuals to be able to prove who they are: in 2018, one billion people in the world lacked access to proof of a legal identity, and a further three billion people who held proof of their legal identities were unable to reliably use them in the digital world.

Broadening access to digital identity systems for individuals can help leapfrog paper-based, resource-intensive and less secure identity systems to propel economic development by opening new markets and including the marginalised into society and the formal economy. Achieving portable and re-usable identity, that works across borders and for both public and private services, can help meet the 21st century needs of citizens and the global digital market.

Digital identity was a vital tool for responding to the COVID-19 pandemic, allowing for the provision of fast, secure, and remote access to public and private sector services. Dramatic increases in adoption followed from its use in aiding epidemiological surveillance, and ensuring the continuity of our societies and economies. As the post-COVID recovery gains pace, digital identity is proving to be critical for enabling the verification of test and vaccination proofs. The benefits witnessed have underscored the importance of leveraging digital identity in future emergencies and crises, and to uphold public trust in digital identity systems by maintaining high security controls and privacy safeguards.

The G20 is well placed to lead a global transition to digital identity. Learning from existing, sometimes fragmented, digital identity solutions in the world and building on its accelerated adoption during the pandemic, the G20 can explore how to ensure that digital identity delivers on its promise of serving a better, more inclusive and prosperous world.

In line with the ambition of the Italian G20 Presidency, this report acts as a descriptive guide to the experience of digital identity for individuals and a potential departure for future work to realise the opportunities offered by portable and re-usable digital identity in the 21st century. Built on a collection of digital identity practices shared by the membership of the G20 DETF, it provides the policy and normative context for digital identity and what this implies, both in terms of challenges and opportunities. It surfaces uses of digital identity during the COVID-19 crisis and considers the necessary enabling conditions for successful adoption of portable and re-usable digital identity.

This report provides four main concluding observations for the G20 membership to support the general development of inclusive, equitable and trusted digital identity solutions that allow citizens to verify and authenticate their identity as easily as possible in any given context:

- **Digital identity can add the greatest value when it is integrated into the day-to-day life of citizens** allowing access to services provided by multiple sectors and countries.
- **It is valuable to continuously reflect on the user experience** (including end-users and service providers) in the development and delivery of digital identity solutions.

- **Digital identity can provide citizens with ownership and visibility of how their data is being used and shared** in order to encourage them to take greater control over their digital identity and to uphold trust in new and existing digital identity systems.
- **The success of digital identity solutions requires a comprehensive governance** grounded on effective legal frameworks, leadership, cross-sector collaboration and resources.

1 Policy and normative context for Digital Identity

Digital identity – easily usable, reliable, secure, trusted, and portable digital identity solutions fit for the 21st century

In 2020-2021, the social and economic impact of the COVID-19 pandemic highlighted the potential value and application of digital identity for individuals[1]. The pandemic accelerated the digital transformation of governments as public services operating in full digital mode meant rethinking how to verify the identity of users. To keep societies open and functional, countries turned to the verification of individual identity to trace contacts, prove vaccination or test status, and support continued international travel. These experiences surfaced the critical importance of maintaining trust in the way governments handle and use the most sensitive data of their citizens[2].

The verification of people's identity has long been core to human and economic development. The sharing of attributes and qualities that make up one person in legal terms is the basis for taking an active role in society, including the ability to vote, interact with government, and receive health care, education and transfer funds. The identification of individuals is also a fundamental right. As enshrined in the Universal Declaration of Human Rights and the International Covenant on Civil and Political Rights, all individuals have the right to be recognised as a person before the law.

Despite recognising the importance of legal identification, the global community still faces big challenges in securing its implementation. The World Bank's Identification for Development (ID4D) Global Dataset reports that worldwide, one billion people lack a proof of identity[3], while a further 3 billion people face considerable limits on the ability to use their proofs of identity in a digital context. The inability for individuals to prove that they exist, and that they are who they are, poses a severe threat to global social and economic inclusion. In 2015, the international community recognised the need to address the issue by adopting Goal 16:9 of the Sustainable Development Agenda 2030 to "provide legal identity for all including free birth registrations". The World Bank Identity for Development 2020 Annual Report[4] emphasised the urgency of the global identity gap, highlighting that it "disproportionately affects vulnerable populations, such as the poor, people living in rural and remote areas, marginalized women and children, stateless persons, migrants, and persons with disabilities." The overrepresentation of vulnerable groups in

[1] Following the request of the G20 membership this report focuses on the experience of digital identity solutions for individuals. Nevertheless, the annex detailing the returns from countries includes examples where consideration has been given to the challenge of identity for organisations and legal entities.

[2] https://www.oecd.org/coronavirus/policy-responses/tracking-and-tracing-covid-protecting-privacy-and-data-while-using-apps-and-biometrics-8f394636/

[3] https://id4d.worldbank.org/global-dataset/visualization

[4] http://documents1.worldbank.org/curated/en/625371611951876490/pdf/Identification-for-Development-ID4D-2020-Annual-Report.pdf

the global identity gap threatens to widen already existing inequalities as societies and economies become more dependent on digital identity verification to effectively function and operate.

There are however, two fundamental promises offered by achieving an equitable and inclusive model for digital identity:

- The first is in addressing the global identity gap by enabling developing countries to leapfrog analogue, resource-consuming identification systems. The Global System for Mobile Communications Association (GSMA)[5], which represents the interests of mobile operators worldwide, has shown a rapid growth of access to mobile broadband worldwide, including across developing countries. Mobile networks are a key enabler of digital identification with mobile network providers (MNOs) and the mobile industry central for helping governments achieve digital identity coverage.
- The second, in line with the ambitious demands of the G20 Digital Government Principles[6] and the OECD Recommendation of the Council on Digital Government Strategies[7], is the transformative potential of easy to use and trusted digital identity solutions to facilitate the way in which services are designed, delivered, consumed and experienced. The challenge facing governments and private sector organisations is not merely to transfer analogue identity systems online but to redesign and rethink interactions between citizens and the state, between non-citizens and authorities, and between consumers and private service providers. In this way, digital identity can be the vehicle for meeting citizen needs through the design and delivery of proactive services as discussed in the *G20 Compendium on the Use of Digital Tools for Public Service Continuity* and section 2 of this report.

Ensuring citizen consent, personal data protection, and security

The combination of new technologies and the handling of sensitive aspects of an individual's very being mean that identity systems are highly scrutinised by the public and civil society and require governments to ensure they mitigate potential risks. The G20 membership, through the Declaration of G20 Digital Ministers, supports the development of digital identity solutions that are based on the users' freely given, specific, and informed consent, and protect citizens' privacy and personal data within the domestically applicable legal frameworks. It further recognizes that receiving government services by means of digital identity should not completely replace other means of accessing services, in order for citizens to meaningfully consent to the use of digital identity. To encourage use and maintain trust in digital identity systems, the practical steps to unlock the potential of digital identity should be built on the existing efforts of international organisations and standard-setting bodies to guide the conversation around digital identity

[5] Commercially Sustainable Roles for Mobile Operators in Digital ID Ecosystems https://www.gsma.com/mobilefordevelopment/wp-content/uploads/2021/03/Commercially-Sustainable-Roles-for-Mobile-Operators-in-Digital-ID-Ecosystems.pdf

[6] G20 Digital Government Principles http://www.g20.utoronto.ca/2018/2018-08-24-digital.html#annex1

[7] OECD Recommendation on Digital Government Strategies https://legalinstruments.oecd.org/en/instruments/OECD-LEGAL-0406

in terms of authentication[8], personal data protection[9] and security risks[10]. It would also benefit from building on previous work of the G20, such as the G20 Digital Identity Onboarding[11] developed under the 2018 Argentine Presidency, which provided a comprehensive documentation of the challenges and opportunities related to digital identity for financial services.

Empowering citizens to take control over their digital identity

Solving the problem of identity verification on the internet has taken many forms since it became apparent that the same needs for verifying the identity of individuals in physical space also existed online. Digital identity is now seen as one of the most important instruments for closing the identity gap in countries where legal identity is not widely accessible. Over time, approaches towards digital identity have shifted focus away from primarily meeting the needs of organisations for authentication, towards empowering citizens with greater control and visibility over their digital footprints with a range of country experiences compared and contrasted by the OECD in 2018[12].

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

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

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

[8]OECD Recommendation on Electronic Authentication https://legalinstruments.oecd.org/en/instruments/OECD-LEGAL-03532002

[9] OECD Privacy Guidelines https://legalinstruments.oecd.org/en/instruments/OECD-LEGAL-0188 and OECD Good Practice Principles of Data Ethics in the Public Sector https://www.oecd.org/gov/digital-government/good-practice-principles-for-data-ethics-in-the-public-sector.htm

[10]OECD Recommendation on Digital Security Risk Management https://legalinstruments.oecd.org/en/instruments/OECD-LEGAL-0415

[11]G20 Digital Identity Onboarding http://documents1.worldbank.org/curated/en/362991536649062411/pdf/129861WP-10-9-2018-17-26-21-GDigitalIdentityOnboardingReportlowres.pdf

[12] Digital Government in Chile – Digital Identity (OECD, 2019), https://dx.doi.org/10.1787/9ecba35e-en compared the experience of 13 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

organisation specific, centralised approaches, a federated model for digital identity was developed as an alternative.

In a federated identity model, a digital identity is not provided by service-specific providers or a single, central solution but through defined trust frameworks and identity standards. These frameworks and standards encourage multiple actors to operate as identity providers (IdPs). Users verify their identity with their choice of IdP and refer to them when they need to access a service requiring identify verification. For those societies without an analogue identity infrastructure of population registers or identity cards, this has become the preferred route to develop digital identity solutions. Federated approaches help to avoid individual organisations developing authentication infrastructure independently, and thus reduces the fragmentation of ownership and responsibility for citizen credentials. Nevertheless, despite its benefits, the federated approach does leave IdPs with a lot of responsibility and control over individuals' identity and their sensitive data[13].

There are increasing calls for digital identity solutions to address the lack of control citizens have over their online identity and credentials. In the 2030 Digital Compass[14], the EU Commission presented their vision for 2030 with a "wide deployment of a trusted, user-controlled identity, allowing each citizen to control their own online interactions and presence". This idea is also at the heart of the EU Commission's proposed regulation in June 2021 to establish the European Digital Identity Framework[15]. Its aim is to realise the vision of a secure and trusted EU Digital Identity available to every EU citizen, resident, and business who wants to identify themselves or provide confirmation of certain personal information online and offline, across public and private services within the EU. All citizens and residents in the Union will be able to use a personal digital wallet, which is already a feature for several countries including Spain, where the associated consent models give individuals greater control and visibility over their data access and use.

Other, emergent ideas favour a more minimal approach to the exchange of personal information and rely instead on the possibilities and potential of decentralising identity to the individual through Self-Sovereign Identity (SSI) and verifiable credentials. These models give citizens ultimate control and ownership over their online presence and each interaction with their digital identity, from what of their attributes and data are being shared, with whom and for what purpose.

Equipping citizens with a portable digital identity they can use anywhere and for anything

Digital identity has the potential to be an important driver of citizen well-being[16]. However, for this potential to be realised it is critical to conceive of digital identity as a service that can equip citizens to address the needs they have in any context and at any time and not as a top-down mechanism for identity verification. Therefore, it is a primary goal for digital identity efforts to achieve as broad and varied portability as possible.

---

[13] As an example, the provision of a version of federated identity with lower levels of assurance that offers simple and ubiquitous log-in and sign-up by large online platforms such as Google and Facebook has become a familiar feature in many citizens' lives, but with the platforms ultimately controlling the user data and associated credentials across the different services they provide access to.

[14] https://digital-strategy.ec.europa.eu/en/policies/digital-compass

[15] Proposal for a Regulation of the European Parliament and of the Council amending Regulation (EU) No 910/2014 as regards establishing a framework for a European Digital Identity (SEC(2021) 228 final). Available at: https://digital-strategy.ec.europa.eu/en/library/trusted-and-secure-european-e-id-regulation

[16] The impact of Digital Government on citizen well-being, OECD Working Papers on Public Governance, (Welby, 2019) https://doi.org/10.1787/24bac82f-en

Portability of digital identity can reflect several important priorities, all of which require their own strategic and practical efforts to fully deliver on their benefits.

Firstly, that a digital identity can be used away from a desk at home or the office. In other words, that access is not restricted only through the presence of suitable hardware such as card readers or digital certificates but can be portable in the sense that someone is able to take advantage of their identity whenever, and wherever they are through an approach to digital identity supported through mobile devices. This necessitates governments to consider the broader implications of policies focusing on connectivity or mobile network coverage to support the development of successful digital identity.

Secondly, that a digital identity can be used in any transactions or interactions that require a high level of assurance, regardless of whether the service is being provided by the public sector, or the private sector. Although the private sector may be involved in providing identity, it is essential to recognise the role of the private sector as a provider of services too. Although the public sector need for digital identity is vital for the design and delivery of services associated with taxation, welfare and health, individuals have similar needs to prove identity in dealings with suppliers ranging from telecommunications, to banking, to travel. The portability of identity between different domains is an important benefit that helps to encourage adoption and ensure the benefits of digital identity are as widespread as possible. In Europe, the newly proposed regulation for establishing an EU Digital Identity Framework has as one of its aims making it easier for users to access more services, irrespective of the type of provider across the single market and reflects the difficulties experienced by private sector service providers in connecting to the digital identity solutions previously developed by Member States.

Thirdly, that a digital identity can be used across geographic boundaries. The ability for individuals to identify themselves outside the jurisdiction in which they reside opens up incredible possibilities for services to be offered across borders and for countries to tailor their response to the needs of users who are neither nationals nor residents, without needing to undertake separate efforts to prove their eligibility or otherwise.

In a domestic context a cross-platform, sector-agnostic digital identity requires agreement on a standards-based approach to unlock the potential value through technical interoperability. However, to extend the portability and reuse of digital identity across borders requires international cooperation and mutual recognition by one country of the solutions that are trusted and supported by another. In April 2021, the UN Commission on International Trade Law (UNCITRAL) published the Draft Provisions on the Use and Cross-Border Recognition of Identity Management and Trust Services[17] with the aim to promote uniformity in the development and application of operational rules, policies and practices for identity management. The principles are applicable in the context of commercial activities and trade-related services. For cross-border recognition, the draft principles says that “An Identity Management system operated or a trust service provided outside [the enacting jurisdiction] shall have the same legal effect in [the enacting jurisdiction] as an IdM system operated or a trust service provided in [the enacting jurisdiction] if it offers a substantially equivalent level of reliability.”

In order to define “substantially equivalent level of reliability” the draft principles point towards recognised international standards and enacting jurisdictions to determinate equivalency. The eIDAS regulation of the European Union remains the best-known practical example of a cross-border recognised digital identity, and thus stands as an important international reference. Currently only mandatory for public services, the system is built as a federated model that provides mutual recognition of each Member State’s national eIDs. Since digital identity is a national competence of Member States, eIDAS addressed the issue of reliability, comparability and interoperability of national digital identities - similar to ensuring “substantially equivalent level of reliability” in the UNCITRAL draft principles - by introducing a detailed technical specification criteria for defining assurance levels, as set forth in implementing regulation (EU) 2015/1502.

[17] https://undocs.org/en/A/CN.9/WG.IV/WP.167

In June 2021, the EU Commission published a proposal for a regulation to amend the current eIDAS regulation in order to foster greater cross-sectoral and cross-border usability within the EU single market and to allow citizens to take greater control over their identity and data.

UNCITRAL and EU activities considering the development and then reuse and availability of digital identity across borders are the main reference materials. However, it is important to recognise multilateral efforts taking place in other parts of the world to achieve cross-border mutual recognition of digital identity such as the work happening between Australia, New Zealand and Singapore as well as further nascent attempts to guide this conversation in regional terms whether in East Africa, Latin America or South-East Asia.

These concerted efforts make the ambition for an ability to move with one's identity across borders an increasingly likely possibility. Nevertheless, this raises interesting questions about the character of future society and the reasons why countries and individuals would wish to pursue such an approach to digital identity. In order to achieve this vision of a portable digital identity that can be used anywhere, and for everything, the challenge is to secure interoperability, reliability and equivalency between different digital identity systems and solutions. Just as with federated and decentralised identity systems, portability calls for enhanced coordination, collaboration and trust between actors of the identity ecosystem with the international angle providing an even greater challenge to overcome that the G20 is well positioned to help facilitate.

Restoring identity to the marginalised and forgotten

The primary focus for conversations about digital identity is usually located in the experience of stable citizenship and residency in domestic settings, where the concerns are transforming government services or delivering value to the economy. However, for the one billion people around the world without access to legal identity documents, or the three billion people in the world who can't use theirs effectively in a digital context, this may not speak to the experience of their lives. This may be because they are socially marginalised in a settled society, or facing the trauma and upheaval of being refugees in more fragile contexts. Nevertheless, the UNHCR Strategy on Digital Identity and Inclusion[18] identifies that as digital technologies broaden the concept and understanding of identification processes, governments remain responsible for ensuring the digital inclusion of all citizens and individuals living on their territory.

In the Declaration of G20 Digital Ministers, the G20 membership has declared to pursue further work to find technology solutions for digital identity that are suitable in internet-scarce settings including in humanitarian and emergency scenarios[19]. By doing so, digital identity solutions can be leveraged to secure the human right for all individuals to be recognised everywhere as a person before the law[20], including those who lack access to legal identity documents, such as refugees, forcibly displaced persons, and

[18] UNHCR Strategy on Digital Identity and Inclusion, https://www.unhcr.org/blogs/wp-content/uploads/sites/48/2018/03/2018-02-Digital-Identity_02.pdf

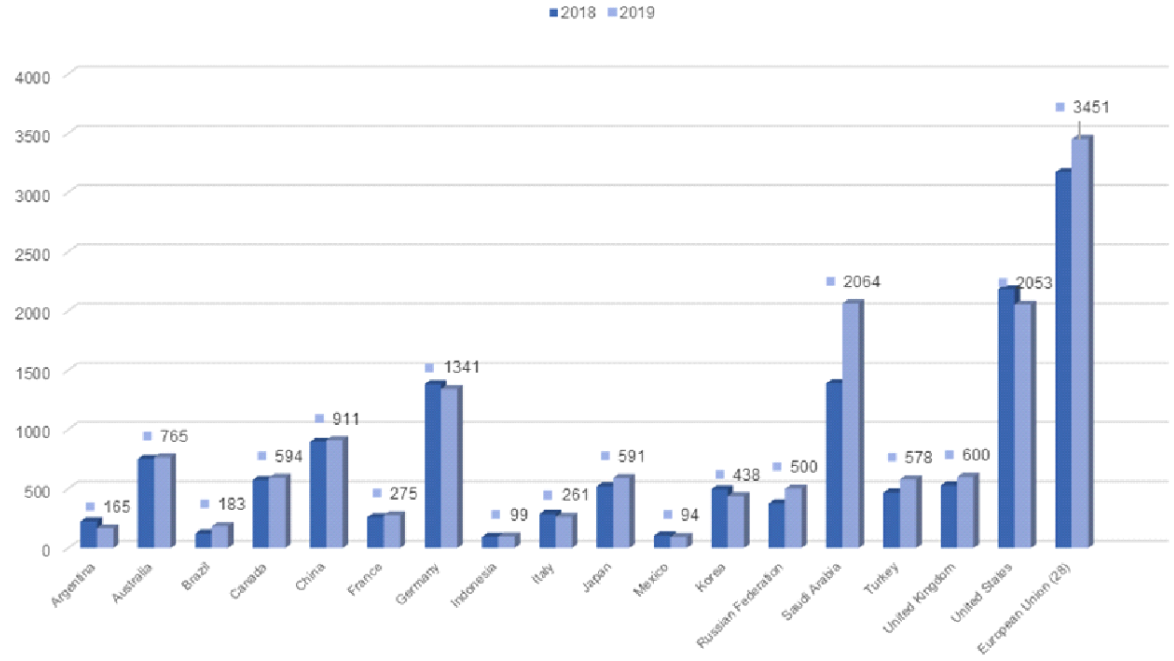
[19] A country that is working on the development of a digital identity solution for refugees is Turkey. The Turkish Ministry of Foreign Affairs and UNDP are piloting a digital identity platform to speed up the process of issuing working permits documentation for refugees. More information is available at https://tykn.tech/turkey/.

[20] Article 6 of the Universal Declaration of Human Rights provides that "Everyone has the right to recognition everywhere as a person before the law." The provision of digital identity solutions is used in identification processes to verify the identity of individuals and provide access to services that require authentication. As such, a digital identity solution can be used to help ensure that individuals are recognised before the law by helping them prove their identity and authenticate themselves without having to access or provide physical legal documents. Having a digital identity does not equal having a legal identity.

individuals living in countries with incomplete civil registration, but also individuals who are financially excluded from society.

Given the large share of the global refugee population hosted by G20 members, the use of digital identity solutions by refugees and forcibly displaced persons in these countries might provide large benefits if carefully developed and implemented. As of mid-2020, UNHCR estimated that the global refugee population was 26.3 million with almost 29% hosted by G20 countries. According to the 2020 Annual International Migration and Forced Displacement Trends and Policies Report to the G20[21], latest available data indicate a 10% increase in migration flows to G20 countries in 2019. When developing and delivering digital identity solutions for humanitarian contexts such as refugee crises, it would benefit from building on previous extensive work of the UNHCR such as the Global Compact on Refugees[22] and consultations hosted at the Global Virtual Summit on Digital Identity for Refugees[23] that contains a set of recommendations concerning digital identity and refugee populations. For the development and delivery of digital identity solutions to address issues of financial exclusion work may build on that of the World Bank in the report G20 Digital Identity Onboarding[24].

Figure 1.1. Migration flows to G20 countries, 2018 and 2019, thousands



Note: Data is not available for South Africa and India. Sources, definitions and coverage of data used vary significantly across countries. This does not allow for aggregations and direct comparisons, but order of magnitude and trends can be described. Data are generally based on national sources, and most often include temporary workers and students. Inflows to Turkey are estimates based on Ministry of Interior and Ministry of Labour reports.

[21] https://www.oecd.org/migration/mig/FINAL-2020-OECD-ILO-UNHCR-IOM-G20-report.pdf

[22] https://www.unhcr.org/the-global-compact-on-refugees.html

[23] https://www.unhcr.org/idecosystem/wp-content/uploads/sites/69/2019/12/Conclusions_and_Recommendations.pdf

[24] http://documents1.worldbank.org/curated/en/362991536649062411/pdf/129861WP-10-9-2018-17-26-21-GDigitalIdentityOnboardingReportlowres.pdf

Source: Graph based on Table.1 of the 2020 Annual International Migration and Forced Displacement Trends and Policies Report to the G20, available at: https://www.oecd.org/migration/mig/FINAL-2020-OECD-ILO-UNHCR-IOM-G20-report.pdf. Original source: OECD 2020a National sources; OECD International Migration Database, OAS/OECD (2017) International migration in the Americas - SICREMI, ADBI/ILO/OECD (2020) Building Partnerships for Effectively Managing Labour Migration.

Digital identity is increasingly an essential infrastructure to respond to the needs of the twenty-first century. For governments seeking to reap the full potential of digital technologies in transforming how their national identity systems work and how they deliver to citizens and marginalised communities, they must ensure that equity and inclusiveness are guiding their efforts. Equally important is that whatever technology, partnership or model is deployed, that it empowers citizens to take control over the sharing and reuse of their data and credentials. This provides the foundation for more advanced efforts to equip individuals with a genuinely portable digital identity, built on the ease and simplicity that they might use it in any context, via any platform, for any service and in any country.

This report uses country examples to explore how G20 member countries have embarked on the journey towards digital identity for individuals, how it assisted them in facing the COVID-19 pandemic, and what conclusions can be made for the international community from these observations. Data and examples presented in this report were collected through the *G20 Digital Identity Survey*, administered in May and June 2021. This surfaced the digital identity experiences of Argentina, Australia, Brazil, the European Union, Germany, Indonesia, Italy, Russia, Saudi Arabia, Singapore, Spain, Turkey, and the United Kingdom. Information was also provided by Democratic Republic of Congo and Mexico where digital identity solutions are currently under development while in the United States of America, identities are generated at the local government level and used to create state government level identity credentials rather than there being a single federal solution. Information was not available for Canada, China, France, India, Japan, Korea and South Africa. This provided information is summarised in the Annex.

As this report is a descriptive guide to the experience of digital identity for individuals it can be a potential departure for future work by the G20 to address the challenges and realise the opportunities offered by portable and reusable digital identity in the twenty-first century. Future work could explore agreement, alignment and practicalities between G20 countries on the need for digital identity that can operate across borders, across public and private services, and in any modality.

2 The role of digital identity in responding to COVID-19

The COVID-19 pandemic amplified the need for public and private service providers to verify the identity of natural persons and businesses in the digital space while maintaining high security and privacy protection. The pandemic saw a fundamental change in how economic and governmental actors operate, not because of dedicated strategies or policies, but because there was no other choice. Yet while the transformation from physical to digital occurred at an incredible speed at all levels of society, this disruptiveness also presented risks of leaving people dissatisfied, mistreated or behind. The G20 members have shared concrete examples and experiences from how digital identity enabled the delivery of valuable services during the pandemic.

Examples of uses of digital identity during the COVID-19 pandemic

Many G20 countries saw significant growth in the adoption of digital identity since the start of the pandemic, with an average four-fold increase between 2019 and 2021[25]. While this might not be attributed solely to the pandemic, there is a correlation between a surge in user adoption and the use of digital identity to access pandemic-related services. In addition to these new services, public health measures meant that existing services that relied on in-person authentication could no longer be provided in the physical space, forcing the authentication process to go digital as well.

Enabling proactive continuity of existing public and private sector services

Brazil saw a significant increase in adoption of digital identity during the pandemic as it was a requirement for accessing the services provided through GOV.BR, the government's single website. The number of available services more than doubled during the pandemic to over 3 000 and saw citizens preferring the digital approach instead of unnecessary social contact during the pandemic. A similar reliance on digital identity was reported in Italy where the IO app, launched in 2020 as a means of accessing local and federal public services, requires the use of either SPID or the electronic identity card CIE and consequently helped support a 269% increase in digital identity adoption among the population between 2019 and 2021.

In other countries citizens benefitted from digital identity to consume private sector services such as in Germany, where individuals could use the eID to prove their identity for activating SIM or eSIM cards remotely without the need for confirming their identity through video calls. In Saudi Arabia, almost all sectors, including health services, commercial, retail, ICT, and the judiciary benefited from digital identity to meet needs during the pandemic.

[25] Average increase in digital identity adoption among population in Germany, Italy, Saudi Arabia, Australia, Turkey, the United Kingdom and Brazil between April 2019 and April 2021. See chapter 3 and Annex for more details per country.

Welfare payments and financial aid

Given the negative economic impact of the pandemic on workers, families and businesses, financial aid has been one of the primary use cases for digital identity solutions. Digital identity was an essential tool for facilitating financial aid for businesses in both Australia and Germany but its most common use was for supporting individuals. In India, the government program for transferring cash subsidies and benefits "Direct Benefit Transfer (DBT)" relies largely on Aadhaar, the country's biometric digital identity system for validating and transferring benefits to beneficiary accounts. In 2020, DBT dispersed benefits for over 400 schemes under 56 ministries, and in October 2020, a total of 47 million beneficiaries received DBT relief up to 140 billion INR[26]. In Argentina, the long-standing commitment to digital identity meant that millions of citizens were able to receive financial support from the state, even during a period of restricted movement. In Italy, the use of the Public Digital Identity System (SPID) for accessing welfare measures as part of COVID-19 recovery packages significantly promoted its uptake.

Contact tracing and lockdowns

Another use of digital identity during the pandemic was to confirm the COVID-19 risk status of individuals in order to uphold public health measures and prevent the spread of the virus, particularly in the use of apps. In Turkey, citizens used their digital identity to log in to the e-Government Gateway and generate a personal code to access the government application "Hayat Eve Sığar – Life Fits Into Home". This code enabled them to safely transfer data about their COVID-19 risk status in order to access services such as public transport and common public spaces.

In Singapore, the national digital identity programme supported the contact tracing processes through the app "SafeEntry", which enables authorised contact tracers to obtain identity information of visitors to a physical location. The identity information processed through the app was used as a credible reference to uncover locations visited by confirmed cases, identify possible clusters and target locations for deep cleaning. In order to use SafeEntry, users give their consent to the transfer of personal information upon scanning a SafeEntry QR code to check in whenever they visit a location. Italy also relied on its digital identity system to facilitate contact tracing efforts via the app "Immuni".

Vaccination distribution and certificates

Distributing vaccines and issuing certificates proving vaccination status have been central to countries' recovery strategies. As governments sought ways to return to normal and facilitate the opening up of borders and services, digital identity again came to play an important part.

In Australia, citizens can use their digital identity to log in to myGov, which provides access to their COVID-19 Vaccination Certificates. Australia's strong authentication and verification methods built into the digital identity system help guard against fraud and ensure the person applying for the certificate is who they say they are. These approaches could form the basis for enabling a strong, internationally recognised and interoperable COVID-19 Vaccination Certificate to support international travel through integration of a person's Digital Identity and digital wallet. In the EU, the EU Digital COVID-19 Certificate was delivered in July 2021. The vaccination certificate allows Member States to more easily confirm the vaccination status of visiting EU citizens. While the certificate does not affect the right of EU citizens to travel freely within the EU borders, it will be able to facilitate the process of EU citizens to enter into a country given the rules and restrictions that are applicable. In some places, this might imply that the individuals holding the certificate do not have to confine themselves upon arrival.

[26] National Informatics Centre blogs, "Direct Debit Transfer – A blessing during the pandemic", https://www.nic.in/blogs/direct-benefit-transfer-a-blessing-during-the-time-of-pandemic/

Lessons learned from the use of digital identity during the COVID-19 pandemic

Given the sensitive types of data collected in order to verify and authenticate individuals' identity for use in pandemic-related services and measures, the upholding of data privacy, data security and considerations for the ethical use of data has been critical in order to reduce the risks of potential harms and data misuse.

Promoting and maintaining trust in digital identity systems

In Australia, the government's digital identity system maintained strong security controls and privacy safeguards to protect user privacy throughout the COVID-19 pandemic. According to the government, there have been no instances identified where the system has been unable to protect user privacy. Likewise, in Turkey the government reports that user privacy has been well protected during the COVID-19 pandemic. Furthermore, Argentina reflected that with an increased reliance on digital tools and remote authentication it is essential to minimise fraud and exposure of personal data and that this underlined the value to the country of centrally developing the Central Electronic Authentication Platform (AUTENTICAR) platform.

Other countries implemented new, temporary laws to facilitate the use of sensitive personal information for public health measures during the pandemic, which may have both a positive and negative impact on the trust associated with digital identity systems. In Singapore, the rules for processing personal data for contact tracing are specified in the Singaporean COVID (Temporary Measures) Act. The act allows public sector organisations and contact tracers to use personal data recorded in digital contact tracing systems only for the purpose of carrying out contact tracing, except where such data is needed by law enforcement for criminal investigations related to seven categories of serious offences, which cannot be modified without parliamentary approval.

The role of digital identity in emergencies and crises

The COVID-19 pandemic will not be the only crisis where it is important for individuals to prove their identity and access services in a fast and secure way without the need for providing physical documents. The Australian Government highlighted how digital identity can provide essential support in the case of natural disasters, as demonstrated during the 2019-2020 Australian bushfires. Digital identities can offset the challenge of finding identity documents such as birth certificates or passports which may have been destroyed, allowing for faster access to government services and relief payments. These benefits apply to any disaster or complex emergencies where people have lost access to physical legal identity documents, or cannot have easy physical access to service providers, which includes the plight of refugees as discussed in Section 1.

3 Enabling the conditions for successful digital identity

Collection of digital identity practices across the G20 membership

Across the G20, there are varied efforts to achieve the successful implementation of digital identity. These differing experiences build on country specific legacy practices and the existing building blocks that go with them. Approaches to digital identity are not universal and therefore it is unwise to attempt to establish a narrative that signals any particular norm for other countries to follow or, indeed, how to define 'success' in the context of digital identity.

Nevertheless, as the experience of digital identity during the COVID-19 pandemic has shown, digital identity is an enabler for societies to thrive in the digital age. Its value is not just limited to moving quickly in a crisis but is directly connected to the extent to which countries can take advantage of the potential for digital transformation. As such, countries can learn from one another about how they approach particular challenges in the implementation and development of digital identity solutions. Based on the responses from the G20 membership to a survey[27], this paper draws out their experience in five areas:

- Governance and funding of digital identity solutions
- The user experience of digital identity solutions
- The role of digital identity solutions in protecting data, handling consent and empowering citizens
- Understanding the adoption of digital identity solutions
- The portability of digital identity solutions across technical platforms, service providing sectors and between different geographic jurisdictions

The successful implementation of digital identity relies on a holistic and coordinated approach. This data capture exercise is intended to document the experience of digital identity across the G20 membership and provide the material to discuss different approaches and lessons learnt rather than to make any recommendations about particular practices. Table 3.1 provides a summary of the digital identity solutions captured through the data collection exercise.

[27] Responses to the survey were received from Argentina, Australia, Brazil, the European Union, Germany, Indonesia, Italy, Mexico, Russia, Saudi Arabia, Turkey and the United Kingdom. The United States provided information through a separate statement. G20 guest countries the Democratic Republic of Congo, Singapore and Spain also responded to the survey.

Table 3.1. National digital identity solution covered in the data capture

	National digital identity
Argentina	SID (Sistema de Identidad Digital) biometric identity platform
Australia	myGOV identity platform
Brazil	GOV.BR identity platform
Germany	German Citizen identity card Electronic residence permit for non-citizens of EU/EEA area eID card for EU citizens
Italy	Public Sector Digital Identity System (SPID) Electronic Identity Card (CIE) National Services Card (CNS)
Indonesia	Single Identity Number
Russia	Unified Identification and Authentication System (USIA)
Saudi Arabia	Digital ID via Tawakkalna and Absher apps
Singapore	Singpass and Corppass
Spain	Electronic National Identity Document (DNIe)
Turkey	e-Government Gateway identity platform
United Kingdom	GOV.UK Verify

Note: Information was also provided by Democratic Republic of Congo and Mexico where digital identity solutions are currently under development while in the United States of America, identities are generated at the local government level and used to create state government level identity credentials rather than there being a single federal solution. Information is not available for Canada, China, France, India, Japan, Korea and South Africa.
Source: OECD (2021), "G20 Digital Identity Survey", desk research.

Governance and funding of digital identity solutions

Realising the potential of digital for government relies on effective governance models[28]. In the context of digital identity, the foundational pillars to support its development, delivery and management include providing strategic leadership and overseeing delivery, securing funding, the design of the model for digital identity and ensuring compliance with identity standards.

Strategic leadership and delivery oversight

The way a country approaches digital identity has far reaching consequences and implications for fundamental elements of how a society functions. It is therefore imperative that digital identity solutions are trusted by service providers as well as being understood and embraced by the public themselves. Achieving the successful technical implementation of digital identity may involve rationalising existing identity infrastructure (such as identity cards) and previous solutions developed on an organisational or sectoral basis. As such, providing visionary and strategic leadership to oversee delivery is critical for successful digital identity.

The design and delivery of digital government activity benefits from proximity and coordination between strategic, delivery and operational actors. Indeed, the majority of surveyed countries place the strategic responsibility for digital identity and its delivery within organisations focused on the digital transformation of government. These organisations include the Digital Transformation Agency in Australia, Department of Digital Transformation in collaboration with Agenzia per l'Italia Digitale in Italy, the Saudi Data and Artificial Intelligence Authority in Saudi Arabia and the Government Digital Service in the United Kingdom.

In Brazil, responsibility for delivery of digital identity rests with the Special Secretariat for Modernization of the State with strategic leadership coming from the Ministry of Economy while in Spain oversight is handled jointly by the Ministry of Economy and Ministry of the Interior. In Argentina, several actors are involved.

[28] OECD (2014), Recommendation of the Council on Digital Government Strategies

The Secretariat of Public Innovation (SIP) from the Chief of Cabinet of Minister's Office establishes the strategic direction and regulatory proposals, the Undersecretariat of Administrative Innovation (located within SIP) implements technical digital identity solutions, and the Ministry of Interior takes operational responsibility for identifying individuals through the National Registry of People (*Registro Nacional de las Personas*, RENAPER).

Some countries have entrusted the delivery of digital identity to state-owned enterprises. In Turkey, the publicly funded satellite operator Türksat is responsible for managing digital identity under the umbrella of the e-Government Gateway. In Germany, strategic leadership for digital identity belongs to the Ministry of the Interior but a state-owned enterprise, the Bundesdruckerei Group, produces documents and devices for secure identification and offers corresponding services, including the three digital identification cards.

Contemporary approaches to digital identity are heavily shaped by the historic context in a given country and these strategic organisations need sufficient mandate to be able to address potential challenges. In some settings, such as Australia, the approach is to develop clear policy positions, set out best practices and design trust frameworks to take advantage of the opportunities for interoperable digital identity. Elsewhere, a stronger legal basis is preferred with Mexico developing new legislation to target the landscape of existing legacy solutions and Brazil using Law nº 13.444/2017 to give digital identity the status of a legal identity for Brazilians to access both public and private sector services.

Securing funding for digital identity and its associated ecosystem

Funding for digital identity has to consider several factors, including initial start-up costs, return on investment and benefits realisation, technical solution development, technical support for relying parties, and whether or not to subsidise access for citizens. In countries where the private sector is a delivery partner, additional costs may be involved to support their role, as well as the creation of a market for digital identity provision.

A majority of countries, including Argentina, Australia, Brazil, Spain and Singapore reported that the provision of digital identity was fully funded by the government. In Australia, this may change in the future as a charging framework is being considered as a means of addressing the long-term sustainability of the system. In Brazil, the budget and technical development for digital identity are centralized within the Secretariat of Digital Government of the Ministry of Economy, which offers a technical team to support public agencies in implementing the digital identity solutions.

In some countries, there is a mixed approach of public funding and funding from external sources, including from financial institutions and identity providers (IdPs) selling their digital identity solutions to service providers. In Turkey, IdPs are financed by the government and by financial institutions. In Saudi Arabia, the government funds IdPs to provide services to the public sector free of charge, whereas private IdPs brokers are self-funded by generating revenues.

Funding models can also be informed by the design of the digital identity solution. For example, in Italy, SPID and its IdPs are self-funding by selling SPID to relying parties whereas the alternative CIE sees users pay approximately EUR 24 to get their identity card with a fraction of this fee used to sustain services provided by the Ministry of the Interior. In some cases, the costs are borne by users with the three electronic identity cards offered in Germany being funded by charging a one-time fee for their production.

Establishing the operational model for digital identity

Governments play an active role in building the identity footprint of an individual whether through their registration at birth, the issuing of identity documents like passports, or documenting someone's relationship with the state for taxation, welfare or responsibility for a vehicle. As a result, the public sector is often a rich source of identity materials. It is therefore no surprise to see a majority of countries indicating a leading role for the public sector in the governance and provision of national digital identity solutions.

In Argentina, Germany, Russia, Singapore and Spain, the model for digital identity relies on the public sector as the foundational actor in providing the basis for an issued digital identity. In Italy, the development of digital identity reflects a partnership between public and private sectors. Along these lines, Indonesia has collaborated with over 3 000 public and private stakeholders to integrate, verify, and validate data in the implementation of digital identity. Although these digital identities come from the public sector, all these countries ensure its availability and usage for accessing private sector services as one option among others. In Argentina and Singapore, the approach is even stronger with a public sector provided digital identity solution being relied on by both the public and private sectors.

Several countries make use of biometrics as part of their digital identity solutions but solely biometric solutions are rare with only India's Aardhaar system and Argentina's SID entirely reliant on biometrics. In both countries, digital identity is an essential tool for citizens and enjoys near universal levels of adoption with the solutions embedded into services provided by both the public and private sectors.

Australia, Italy and the United Kingdom are pursuing a federated model of digital identity. Under a federated approach identity infrastructure is not run by the government and users do not rely on a singular identity provided by the government. Instead, users register with an appropriate identity provider (IdP) who can verify an identity when needed. Under these models, the role of government is oversight and standards setting to cover the user experience and the protocols around identity proofing, verification and authentication. In Australia and Italy, IdPs are drawn from both the public and private sectors while, in the United Kingdom, IdPs are private sector suppliers. Unlike Italy, where SPID can be used for accessing private sector services, the digital identity solutions in Australia and the United Kingdom is limited to the access of public sector services only. However, these countries are actively considering how to expand their trust frameworks to include private sector services too.

Turkey and Brazil have models where the digital identity solution for public services allows users to authenticate using the platforms of large banks, with the motive of promoting the uptake and use of digital services by those who already trust and use their bank's solution. G20 members are open to the active role of non-government actors in the governance and development of digital identity with almost all respondents indicating the involvement of financial service providers and several additionally highlighting the role of telecoms providers and software companies. In Australia, Brazil and Germany there is also recognition of including academia.

Setting standards and levels of assurance for digital identity

No national digital identity solution is created without accounting for the existing identity landscape in a country. For all G20 members, this reflects those public sector efforts that have gone into securely demonstrating identity, whether through analogue means or previous digital efforts. It also needs to acknowledge private sector work for businesses to meet the needs of their customers. This landscape can mean that some services:

- are designed to bypass digital identity by keeping the need for provable identity to a minimum
- require individuals to provide information every time they access the service rather than reusing data held elsewhere
- handle authentication and verification needs through a dedicated account or in issuing specific credentials for accessing specific services
- operate under the basis of an organisational or sectoral approach to identity, for example all services provided for taxation may have a discrete solution for addressing their identity needs
- reuse shared or federated solutions either from elsewhere in government or in provision from the private sector.
- enable the exchange and reuse of verified credentials between existing sources of government data

These different mechanisms for authenticating and verifying users reflect a value in differentiating between levels of assurance. The level of assurance describes the certainty to which a person using a digital identity solution can be trusted to actually be who they claim to be.

The way in which countries define and manage levels of assurance draws on multilateral standards setting bodies such as the European Union (EU) and the International Organization for Standardization (ISO) as well as domestic organisations including the U.S National Institute of Standards and Technology (NIST). The most commonly referenced standards include the EU eIDAS regulation and ISO-IEC 29115 on entity authentication assurance.

These standards set out how to consider the definition in terms of identity proofing and authentication. Identity proofing levels of assurance are informed by factors such as how the initial identification takes place (remotely or in-person) and the attributes that are collected. Authentication levels of assurance determine the quantity of means of authentication (one-factor, two-factor or three-factor) used to confirm that an individual should be given access, the credentials collected and their cryptographic strength. Under NIST's Digital Identity Guidelines (NIST 800-63-3), a third dimension has been added to consider the requirements for identification and authentication in federated environments and focuses on the nature of access to approved cryptography. Several countries, including Australia, Brazil (see Box 3.1), Italy and Singapore have digital identity solutions that make multiple tiers of assurance available, offering flexibility to both users and relying parties.

Box 3.1. Identity proofing on the GOV.BR identity platform, Brazil

In Brazil, citizens can use different methods to complete the online onboarding for a digital identity to access GOV.BR. All methods require citizens to have their tax identification number.

Bronze category

- Based on Knowledge-based Authentication (KBA), citizens must answer personal questions including questions related to their labour and pension records.

Silver Category

- Based on banking authentication, bank customers can, by means of bank digital identity login, identify themselves on the GOV.BR Identity platform.
- Based on facial biometrics saved in the driver's license database citizens can identify themselves using mobile phone cameras.

Gold Category

- Based on facial biometrics stored in the National Civil Identification (ICN) dataset identification can be done using a mobile phone camera. Currently, the database holds biometric data for 118 million Brazilians.
- Citizens can complete the onboarding process through the website address acesso.gov.br and have the support using the app (Meu gov.br) which is available at Google play and Apple Store.

Source: OECD (2021), "G20 Digital Identity Survey"

Higher levels of assurance are suitable where the priority is to minimise risk, but if an interaction is less open to abuse or security critical a lower standard may be applied in order to simplify the user experience. For example, biometric-based authentication provides a higher certainty of a user's identity than many

'ordinary' digital services will require. Ultimately, judging the appropriate level of assurance means finding a balance between mitigating risk and retaining usability in terms of:

- the likelihood that any failure in the authentication process will release sensitive information,
- the damage such a failure would cause to individuals, organisations or public trust
- the overhead to the user (including their exclusion) or the service provider of meeting the requirement in order to access or provide a service.

International standards that shape a global understanding of levels of assurance support countries to develop their own domestic standards for governing digital identity solutions. This is particularly important if the operational model for digital identity involves third parties in the identity proofing and authentication processes. In the United Kingdom, the national identity proofing standards draw on existing global standards and regulations, including the Pan Canadian Trust Framework Model[29], in Italy the government assesses and certifies the quality of private identity providers for SPID through an accreditation process carried out by AgID, and in Australia the National Identity Proofing Guidelines and the Trusted Digital Identity Framework reference international standards to govern the activity of entities involved with delivering elements of the country's digital identity solution.

In Argentina, the biometric model for digital identity is unique amongst the participants in the survey and the most relevant standards that support this approach are drawn entirely from outside the country. The International Civil Aviation Organisation provides the basis for facial recognition and the United States' NIST and Federal Bureau of Investigation do the same for fingerprints.

The EU provides a further helpful illustration of how standards can unlock the opportunity for domestic approaches to digital identity to be usable elsewhere. Most of the digital identity solutions of EU member states are not using a federated model but the eIDAS regulation effectively creates a decentralised model for digital identity in order that 27 different domestic digital identity solutions can be reconciled to allow individual governments to rely on the efforts of their peers. The ambition underpinning eIDAS is for a citizen holding the digital identity of their country to access services provided by another. In June 2021 the European Commission published new proposals, building on the experience of the eIDAS regulation, to reflect developments and evolutions in the digital identity landscape to ensure that where citizens are reusing identity across borders it is as seamless and effective as possible.

User experience

For citizens, the ability to use a single, secure identity solution across services and platforms has the potential to increase the incentives to obtain a digital identity. Several countries have challenges in the implementation of digital identity solutions that result from past efforts to digitise analogue identity processes.

For countries with a national ID card the first e-ID solutions could upgrade these existing models to include smart chips. Although these cards could now hold more extensive information they required card readers to be usable. To overcome these usability challenges public and private sector organisations developed their own technical solutions for identifying and verifying users. Although these were not as robust as the solutions using ID cards a trade-off was made in favour of usability to meet their immediate needs.

The priority given to usability can be seen in Brazil, where the digital identity system integrates with the authentication platforms of large banks. According to their experience, one of the most valuable lessons has been a model based around the idea of "one citizen, one identity and authentication solution for all digital government services". As digital identity becomes ubiquitous in the domestic context, the

[29] Developed by the Digital ID and Authentication Council of Canada (DIACC)

expectation of citizens will increase to allow citizens and businesses to easily prove their identities to access public and private sector services provided across borders, as is imagined by eIDAS in the EU.

Table 3.2. What the national digital identity can be used for

	Authentication for accessing public sector services	Authentication for accessing private sector services	As proof of legal identity
Argentina	X	X	
Australia	X		
Brazil	X		
Germany	X	X	X
Italy	X	X	X
Indonesia	X	X	
Mexico	X		
Russia	X		
Saudi Arabia	X		
Singapore	X	X	
Spain	X	X	X
Turkey	X		
United Kingdom	X		

Note: Information is not available for Canada, China, France, India, Japan, Korea, South Africa and the United States of America. Information was also provided by Democratic Republic of Congo and Mexico where digital identity solutions are currently under development
Source: OECD (2021), "G20 Digital Identity Survey", desk research.

The first step for users to obtain their digital identity is identity proofing. In eight of the surveyed countries, this is possible through an online-only process. When it comes to the user experience of activating a digital identity, security and levels of assurance should be balanced against the ease of the experience for users. Germany does not currently have an online-only process but the Federal Government is developing a Smart-eID solution that will work without creating a physical ID card. The Smart-eID will store the identity data that would be contained in the smart card in a security element or the eSIM of a smartphone. The phone could then be used for identification on the Internet without using the ID card.

Means of authentication

Another important part of providing a seamless user experience of digital identity are the means of authentication individuals and businesses can use. Some of these solutions support the cross-platform ambitions of governments to support mobile devices. Nevertheless, digital identity solutions need to be accessible to all of society and reflect the experience and needs of vulnerable populations, including elderly and disabled people, as well as those with limited access to stable internet.

Smartcards

Five of the surveyed countries use smartcards as a means for authentication and verification with Indonesia considering the potential for its future use. The use of smartcards is often indicative of upgrading physical identity documents rather than rethinking identification processes for cross-sectoral, cross-platform and cross-border use. In Germany, Italy and Spain, the national identity smartcards are acceptable as valid identity documents which can present a challenge in trying to migrate from physical cards to mobile solutions. In Germany and Italy, authentication using smartcards is possible through Near-Field Communication (NFC) enabled smartphones and avoids the need for card reading hardware, however the initial creation of the cards is currently dependent on a face-to-face process although Germany's Smart-eID plans would address this. Having a physical card may help individuals trust their digital identity and

feel greater security and reliability while for others it may be a barrier to adoption due to their frustration of having to carry a physical card.

Digital certificates and e-signatures

Digital certificates provide proof of ownership over a public key, also known as identity certificates or public key infrastructure. Today, digital certificates are being deployed in eight of the surveyed countries. In Spain, the public sector eID gateway Cl@ve which provides access to digital public services allows the use of username and password and digital certificates (including DNIe) for authentication. In Brazil, digital certificates are being used by private sector organisations who access government services from the Brazilian Federal Revenue Office.

The role of e-signatures can be particularly relevant for facilitating business and public sector processes, where qualified e-signatures can be regarded as equivalent to handwritten signatures to prove authorship. This is the case in Germany and Italy, two countries covered by the standards introduced through the EU's eIDAS regulation to ensure the secure and consistent use of e-signatures. In Singapore, 64% of the population that has a digital identity uses e-signatures and each month account for 37 000 authentications. In Argentina, the digital signature is used in applications and official systems of the National Public Service and is facilitated by Remote Digital Signature Platform (PDRF).

Username and password

The most familiar online authentication processes use usernames and passwords and this is a popular approach for digital identity solutions with countries adopting this approach including Brazil, Germany, Italy, Russia, Singapore and Spain. This means of authentication is considered useful for people with basic digital skills and for accessing services where a failure in the identity process would result in a negligible damage. However, while this may be an intuitive approach for some people, there is a reliance on individuals to remember their credentials without storing them insecurely. As such, single-factor authentication solutions offer less protection against fraudulent use of digital identity.

Two-factor authentication

Two-factor authentication (2FA) offers an extra level of security in ensuring the people trying to access a service are who they say they are. 2FA can be a valuable way of increasing security without harming the user experience by removing the need for physical cards or specific hardware. Italy, one of the countries that identified the use of usernames and passwords, increases their level of security by requiring 2FA.

2FA solutions can confirm access to an email account, a mobile phone number or a mobile device or they can involve matching biometric information. A majority of the surveyed countries use 2FA to confirm access to either a mobile phone number or mobile device. In Italy, the use of 2FA to confirm access to a mobile phone number reflects the country's strategy of moving towards an increasingly mobile digital government that values the portability and availability of digital identities on mobile devices.

Biometrics

The introduction of new digital technologies for collecting biometric data, whether facial recognition, iris scanning, voice printing or fingerprinting, has been embraced by six of the surveyed countries as part of their 2FA solutions.

From a user perspective, biometric authentication can be a practical, reliable and fast way to prove identity given that biometric data cannot be forgotten, lost, or easily changed. Yet, for the same reason, there are important challenges in ensuring privacy and citizens' ultimate control over their personal information. This includes the risk of the collected biometric data being used for purposes other than was originally agreed.

The risks and controversy surrounding the use of biometrics require governments and service providers to set up and comply with data management, privacy and data protection protocols, as well as reflect appropriate principles for ethical use[30] in order to safeguard the integrity of the digital identity systems and its end-users.

Argentina is unique among the surveyed countries in having a digital identity solution that is entirely reliant on biometric markers for facial recognition and fingerprint scanning held in the central National Registry of People (*Registro Nacional de las Personas*, RENAPER). Brazil, Germany, Saudi Arabia, Singapore and Turkey also augment their digital identity solutions with biometric information.

Table 3.3. Means for authentication

	Smartcard using a card reader	Digital certificate file or similar	E-signatures	Username and password	2FA email account	2FA mobile phone number	2FA mobile device	2FA biometric information
Argentina			X					X
Australia							X	
Brazil		X		X			X	X
Germany	X	X	X	X	X	X	X	X
Indonesia		X	X					
Italy	X	X	X	X	X	X	X	
Russia			X	X				
Saudi Arabia	X	X				X		X
Singapore		X	X	X		X	X	X
Spain	X	X		X		X		
Turkey	X	X	X	X	X	X	X	X
United Kingdom						X	X	

Note: Information is not available for Canada, China, France, India, Japan, Korea, South Africa and the United States of America. Information was also provided by Democratic Republic of Congo and Mexico where digital identity solutions are currently under development
Source: OECD (2021), "G20 Digital Identity Survey". Information is based on a country's answer to the question "When users in your country access Digital Identity solution(s) for authentication and verification, what methods for authentication does it use?"

Data privacy, visibility and user consent

Digital identity is a potential vulnerability in terms of accessing highly sensitive information about individuals and their lives. To enable the trustworthy adoption of digital identity, and allow for elevating the standards of digital identity around the world, it is non-negotiable for data protection, digital security and citizen consent to be prioritised.

Legislation to protect personal identifiable data and oversight authority

Data protection was a dominant theme in the survey responses with almost all respondents having data protection legislation in place to protect the processing of personal identifiable data in DI systems. In Indonesia where the feasibility for improving digital identity and personal data protection is underway, the intent is to ensure a close working relationship between the two, drawing on international experiences and standards in this area.

[30] OECD Good Practice Principles of Data Ethics in the Public Sector https://www.oecd.org/gov/digital-government/good-practice-principles-for-data-ethics-in-the-public-sector.htm

In countries where there are no single central records with unique personal identifiers, and where this approach is purposefully avoided, as in Australia and the United Kingdom, dedicated trust frameworks can be formed to supplement existing privacy and data protection legislation. In Australia, the Trusted Digital Identity Framework (TDIF) was developed to ensure that personal data entering the Australian Government Digital Identity system is subject to stringent privacy protections. The TDIF contains a number of privacy specific rules, including rules which require accredited participants to:

- conduct privacy impact assessment for high risk changes to their system,
- have privacy officers and privacy champions,
- only use behavioural information in certain ways, and
- seek explicit and informed consent before sharing an individual's attributes with a relying party.

The TDIF has requirements that disallow accredited providers from disclosing a user's data without their consent. It also has requirements that prevent organisations from using personal information for direct marketing purposes.

In order to ensure trust in digital identity systems, there is a need to establish organisations and mechanisms to oversee the impact of digital identity on individual privacy and freedoms, and take appropriate action in case things go wrong. This role is often assigned to National Data Protection Authorities who have a broader mandate than digital identity. In the majority of cases these bodies are independent, have onsite and offsite investigatory and sanctioning powers to safeguard accountability for the appropriate processing of personal data in digital identity systems.

Table 3.4. Authority that monitors and oversees the impact of DI on individual privacy and freedoms

	There is an authority that monitors and oversees the impact of DI on individual privacy and freedoms	The authority is independent	The authority has onsite and offsite investigatory power	The authority has sanctioning power
Argentina	Yes	Yes	No	Yes
Australia	Yes	Yes	-	-
Brazil	Yes	Yes	Yes	Yes
Democratic Republic of Congo	No	-	-	-
Indonesia	Yes	Yes	-	-
Italy	Yes	Yes	Yes	Yes
Mexico	Yes	Yes	Yes	Yes
Russia	Yes	Yes	-	-
Saudi Arabia	Yes	Yes	Yes	Yes
Spain	Yes	Yes	-	-
Turkey	Yes	No	Yes	Yes
United Kingdom	Yes	Yes	Yes	Yes

Note: Information is not available for Canada, China, France, Germany, India, Japan, Korea, Singapore, South Africa and the United States of America.
Source: OECD (2021), "G20 Digital Identity Survey". Information is based on a country's answer to the questions "In your country, is there an authority that monitors and oversees the impact of Digital Identity on individual privacy and freedoms?"; "If yes, is this authority independent?"; "If yes, does this authority have onsite and offsite investigatory power?"; "If yes, does this authority have sanctioning power?"

To overcome the challenges of trust over the use of data, countries are developing models that restrict unnecessary data collection, promote visibility of what data is being processed, and seek consent. In the United States, the federal government is working to recognize identities from the state and local levels to enable secure digital access to federal services while prioritizing privacy, minimizing data collection, and ensuring user consent before data is used or shared. This includes firewalling to ensure that data is not

shared with agencies who do not need access to the data to provide the service requested, as well as avoiding the collection of data to provide a service where that data is not necessary.

In Germany, after the connection between the ID card and the smartphone or the card reader has been established, the user receives information about which provider has requested data and the specific data that is involved. Before any transfer of data the user makes an informed choice about giving their confirmation, or refusing to do so. The issuing authority for authorisation certificates in the Federal Office of Administration grants service providers the state authorisation to read out the identification data from the national online ID when fulfilling the requirements. In Turkey, according to the country's data protection law, natural persons whose personal data are processed have a right to request data to controllers within the scope of their rights specified in law. The law establishes several rights, including knowing whether personal data is processed or not, the purpose of processing data, to whom personal data is transferred, and to request the erasure or destruction of the data. In Singapore, users can access their transaction history in the Singpass app to see what attributes or data are shared, and with whom. When it comes to accessing biometric data, users are required to give consent for their facial image to be compared against the Government's biometric database for authentication purposes.

A further evolution in the approach to digital identity is offered by self-sovereign identity and verifiable credentials. These technologies offers possibilities for empowering users with greater control over their digital identities in deciding what data they want to share, and with whom. Although its use is being explored in Germany, Italy, Saudi Arabia and Spain, none of the surveyed countries have yet implemented such a system.

Table 3.5. Data visibility and consent

	Citizens are proactively informed by authorities about any processing of their personally identifiable data	Users of DI can access and see what attributes or data are being shared/re-used, and with/by whom	Users can provide and revoke consent for the re-use and sharing of attributes or data originating from their DI	Civil society organisations are monitoring the process by which a person's identifiable data is shared and reused
Argentina	No	Yes	Yes	Yes
Australia	No	Yes	Yes	-
Brazil	No	No	No	No
Germany	Yes	Yes	-	No
Italy	Yes	Yes	Yes	No
Mexico	Yes	Yes	Yes	-
Russia	No	Yes	Yes	No
Saudi Arabia	No	No	No	No
Singapore	Yes	Yes	No	-
Spain	Yes	-	Yes	-
Turkey	Yes	Yes	Yes	No
United Kingdom	Yes	Yes	Yes	Yes

Note: Information is not available for Canada, China, France, India, Indonesia, Japan, Korea, South Africa and the United States of America. Information was also provided by Democratic Republic of Congo where digital identity and data protection approaches are currently under development.

Source: OECD (2021), "G20 Digital Identity Survey". Information is based on a country's answer to the question "In your country, are citizens proactively informed by authorities about any processing of their personally identifiable data?"; "In your country, can users of Digital Identity access and see what attributes or data are being shared/re-used, and with/by whom?"; "In your country, can users provide and revoke consent for the re-use and sharing of attributes or data originating from their Digital Identity?"; "In your country, are civil society organisations monitoring the process by which a person's identifiable data is shared and reused?"

Adoption

Underpinning the implementation of digital identity efforts in G20 member countries is the expectation for a digital identity to be adopted and put to use among citizens. Most of the time, high rates of adoption are presented as a measure of success, yet understanding and defining what to measure is complex, especially when comparing countries. Not all citizens or businesses may want or choose to use the available digital identity solution and several countries provide their citizens with the legal right to opt out, meaning that 100% adoption may never be achieved. Within the European Union, the EU Commission has settled on the target of seeing 80% uptake amongst citizens by 2030[31]. In Italy, the Strategy 'Italia 2026' aims at increasing the uptake of digital identity in Italy by 70% of the adult population by 2026.

Mandating use

In some jurisdictions, efforts are focused on making the adoption and use of a particular digital identity mandatory. In Brazil and Saudi Arabia, this mandation is applied to citizens, requiring that they sign up to the specified digital identity solution to access certain services, while in Australia, Germany, Italy, Spain, Turkey, and the United Kingdom, citizens can opt out.

An alternative approach, as seen in Brazil, Germany, Italy, Singapore, Spain and Turkey, is to require that public sector organisations use the specified digital identity solution when designing and delivering public services. Although this appears to effectively mandate citizens to adopt the same digital identity solution, these countries provide alternative solutions for those who have not adopted digital identity themselves.

As part of promoting the uptake of digital identity, many governments provide resources for service providers to facilitate their onboarding. These can include guidelines, training, software and standards. Germany's Federal Ministry of the Interior, Building and Community provides information to authorities on the portal personalausweisportal.de describing how the online identification function can be integrated into processes. This also includes technical information as well as contact details of eID service providers and identification service providers. The Bundesdruckerei Group supports federal authorities that want to establish their own eID infrastructure for electronic identification with the online ID function, by providing a central eID service, the required authorisation certificates and SSL/TLS certificates as well as technical integration into existing IT systems.

In Argentina and Brazil, technical teams exist to support public agencies in implementing the digital identity solutions. In Spain, resources such as integration packages are available and there is support to help the public sector teams. In Spain, the common platform for identification and authentication Cl@ve prevents public sector organisations from having to implement and manage their own identification and signature systems, and citizens having to use different identification methods to interact electronically with the Administration. In Singapore, non-public sector teams can access the Singpass API portal to access resources to onboard onto the various Singpass products. These resources include an API library, onboarding tutorials and guidelines, technical specifications, implementation templates and sandbox APIs to encourage ease of onboarding.

[31] 2030 Digital Compass https://digital-strategy.ec.europa.eu/en/policies/digital-compass

Table 3.6. Mandatory use of available DI solution(s) for service user authentication and verification by public sector organisations

Country	Mandatory
Argentina	No
Australia	No
Brazil	Yes
Germany	Yes
Italy	Yes
Russia	No
Saudi Arabia	Yes
Singapore	Yes
Spain	Yes
Turkey	Yes
United Kingdom	No

Note: Information is not available for Canada, China, France, India, Indonesia, Japan, Korea, Mexico, South Africa and the United States of America. Information was also provided by Democratic Republic of Congo and Mexico where digital identity solutions are currently under development.
Source: OECD (2021), "G20 Digital Identity Survey". Information is based on a country's answer to the question "In your country, is it mandatory for central/federal public sector organisations to use available Digital Identity solution(s) for service user authentication and verification?"

Measuring adoption

The numbers involved with the adoption of digital identity can be highly impressive with Indonesia reporting that the verification process carried out by the country's Ministry of Home Affairs has been completed 7 billion times. However, these numbers are not always so easy to report, particularly where countries have multiple digital identity solutions. For example, in Italy, citizens can have accounts with one, or both, of the SPID or CIE solutions while in the United Kingdom, the GOV.UK Verify model gives citizens the choice of being able to use multiple identity providers as they prefer. By creating an ecosystem of digital identity in this way, citizens have choice and there is flexibility of approaches in using a particular digital identity for some services, and other digital identities for others. This gives greater control to the individual user over their activities but makes it harder to numerate the adoption figures of digital identity.

Efforts to measure adoption can furthermore be misleading as not every public service and not every citizen may require high levels of assurance – for example, obtaining a fishing permit is not the same as securing welfare payments or completing a tax return. Therefore, to understand the adoption of digital identity means considering the opportunities and relevance for digital identity in relation to available public services. As such, there is a need to complement underlying figures with a rounded understanding of the total addressable market in terms of existing digital identity solutions that may be in use as well as the categorisation of available services according to their needs in terms of assurance.

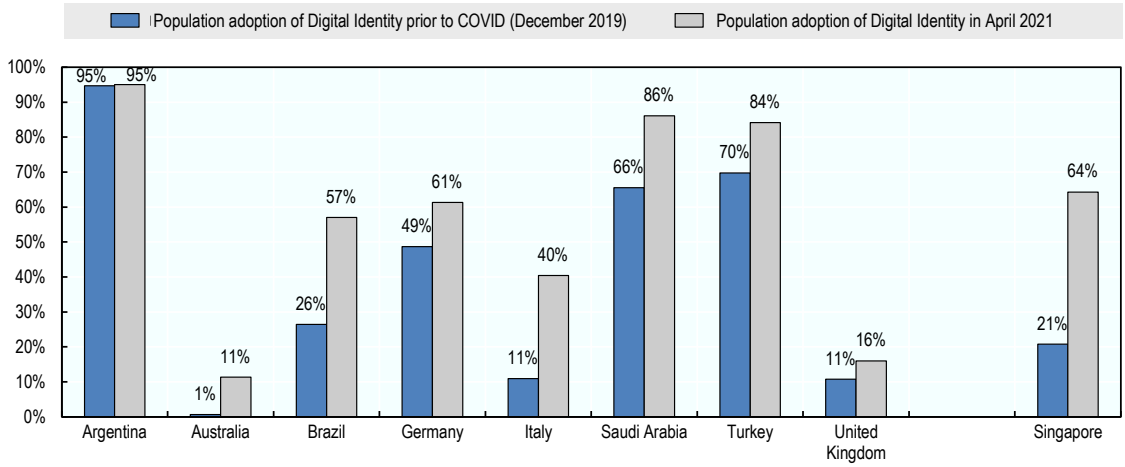
One factor in encouraging adoption is proactively informing the public about the availability of new services accessible with the use of the national digital identity solution. In Italy, during the COVID-19 pandemic, the government used the press, television and social media to share news of COVID-19 recovery packages that could be accessed via digital identity, which resulted in a boost of user adoption.

Another factor is the initial process by which citizens are able to obtain a digital identity. In some countries this is triggered by the citizen having need of a public service and then following through with the sign-up procedure. Where this can be done remotely, as in eight of the surveyed countries, there is no barrier to adoption with users being able to immediately continue with resolving their need. However, if the enrolment process requires proving biometric markers then a face-to-face interaction may be required which can be a stumbling block and a bottleneck for adoption. Under these models, such as that of Argentina, there is merit in encouraging users to activate their digital identity even before they need to use it as well as working to develop solutions for activating a digital identity remotely.

During the COVID-19 pandemic many governments developed new, or extended existing, public services focusing on welfare payments that did require high levels of assurance and, as countries went through extended periods of lockdown and enforced remote interaction, the importance of a reliable and adoptable digital identity solution came to the fore. With mandatory digital identity in place, Argentina could already report 95% adoption rates prior to the pandemic, a situation that allowed for the ready distribution of financial aid throughout the country. However, in the other countries Figure 3.1 shows the significant change occasioned by the pandemic with Italy, Brazil and Singapore reporting the largest percentage point increase between December 2019 and April 2021, ranging from 43 in Singapore, to 29 in Italy. When looking at the percentage increase in adoption, as seen in Figure 3.2, the estimated rate of change in the share of the eligible population with a digital identity is most dramatic in Australia where growth was 1 662%. These increases are linked to the provision of new services on digital platforms, especially in those countries where digital identity solutions support both public and private sector services.

Figure 3.1. Adoption of digital identity among the population, 2019 compared to 2021

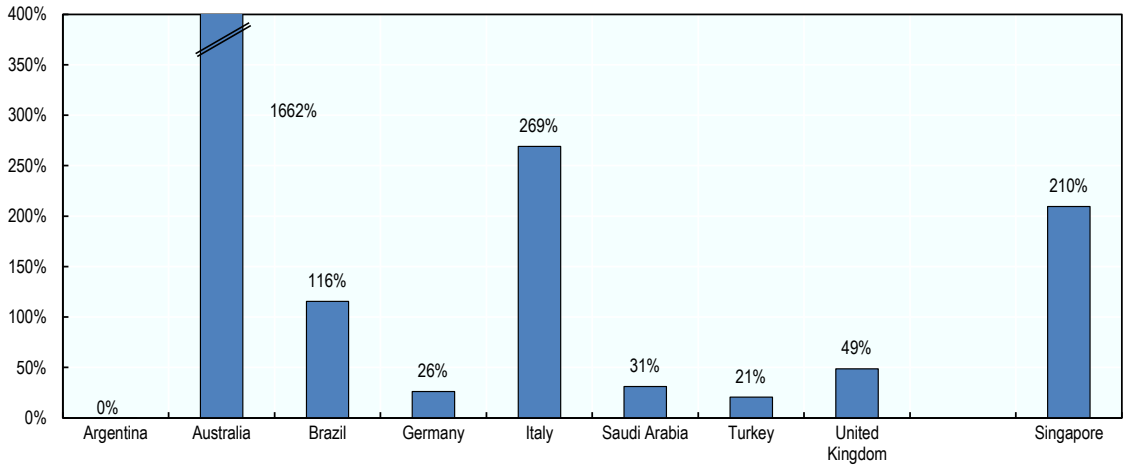
% of eligible population



Note: Data is not available for Canada, China, France, India, Indonesia, Japan, Korea, Mexico, Russia, South Africa and the United States of America. Information was also provided by Democratic Republic of Congo, Indonesia and Mexico where digital identity solutions are currently under development.

Source: OECD (2021), "G20 Digital Identity Survey". Adoption is calculated as a percentage of the eligible population (based on age) with a digital identity, and information is collected from the answer to "What is the youngest age at which someone can have a Digital Identity in your country?" and "The total population in your country that had a Digital Identity on 1st December 2019:" and "The total population in your country that had a Digital Identity on 1stApril 2021:" Data on the total eligible population in the United Kingdom is collected from the UK Office for National Statistics (ONS).

Figure 3.2. Percentage increase in adoption among the population, 2019 compared to 2021



Note: Data is not available for Canada, China, France, India, Indonesia, Japan, Korea, Mexico, Russia, South Africa and the United States of America. Information was also provided by Democratic Republic of Congo, Indonesia and Mexico where digital identity solutions are currently under development.
Source: OECD (2021), "G20 Digital Identity Survey". Calculated based on data collected from country's answer to "What is the youngest age at which someone can have a Digital Identity in your country?" and "The total population in your country that had a Digital Identity on 1st December 2019:" and "The total population in your country that had a Digital Identity on 1st April 2021:" Data on the total eligible population in the United Kingdom is collected from the UK Office for National Statistics (ONS).

Portability

A majority of the surveyed G20 members are working on cross-platform, cross-sectoral and cross-border portability to some extent. Portability is an increasing necessity for the effective use of a digital identity across services, platforms and geographical borders. The way to achieve this may include the need to update regulatory and legal frameworks and to strengthen the basis for cross-border and international identity efforts and collaboration.

Table 3.7. Current levels of portability of digital identity

	Cross-platform	Cross-sectoral	Cross-border
Argentina		X	
Australia	X		
Brazil	X		
Germany	X	X	X
Italy	X	X	X
Russia	X		
Saudi Arabia	X	X	X
Singapore	X	X	
Spain		X	X
Turkey	X		
United Kingdom	X		

Note: Information is not available for Canada, China, France, India, Indonesia, Japan, Korea, Mexico, South Africa and the United States of America.
Source: OECD (2021), "G20 Digital Identity Survey", desk research.

Cross-platform portability

A majority of countries are moving away from smartcard-based models of digital identity as alternative approaches offer improved usability, especially in terms of cross-platform portability. Nine of the surveyed countries enable users to access digital identity through a mobile device which is not device specific. In Italy, SPID can be used through a mobile application on any mobile device and CIE can be used with mobile devices containing Near-Field Communication (NFC) technology. Fully mobile digital identity is a priority for Italy and will involve closer collaboration with Mobile Network Operators. The Australian Government's digital identity system for accessing public service is also available through a mobile application - the myGovID app - on any mobile device and is considered cross-platform portable. The app myGovID can be downloaded on Apple App Store and Google Play.

In Singapore, in addition to the national digital identity for individuals Singpass and the Corporate Digital Identity for businesses Corppass, the government is progressively building a mobile version of a Corporate Digital Identity for businesses. This with the aim to cater for the increasing volume of electronic corporate transactions by introducing a corporate alternative to an individual's digital identity and enabling corporations to leverage the government's digital signature products.

Cross-sectoral portability

There is a growing consensus about the value for citizens and businesses to use digital identity across sectors and services, whether it may be to apply for a loan, complete digital payments, book a doctor's appointment, or declare taxes. However, only 50% of the surveyed countries provide such a cross-sector portable digital identity solution. Argentina, Germany, Italy, Saudi Arabia, Singapore and Spain all reported that their digital identity solution can be used for accessing both public and private sector services.

In Argentina and Singapore, the national digital identity solutions can be used to access both public and private sector services. Non-public sector teams can access the APIs underpinning the solutions in both countries. In Argentina the same level of support for private sector teams is provided as to public sector teams with 24/7 help available. In Singapore, support resources include an API library, onboarding tutorials and guidelines, technical specifications, implementation templates and sandbox APIs to encourage ease of onboarding.

In Italy, while private sector service providers can use the national digital identity SPID to authenticate service users, only between 1-24% are currently doing so. The remaining services are using identification through personal credentials via websites or mobile apps or in-person identification through paper documents. The case of Italy points to the fact that promoting the onboarding of service providers is equally important as providing a cross-sectoral identity solution and this requires having a complete view of the market of available identity solutions.

Cross-border portability

The ability to use digital identities across geographical boundaries and borders has been raised a priority by the G20 membership, and several countries are looking into developing mutually recognised digital identities through trust frameworks, internationally recognised standards as well as new technologies that can help facilitate its realisation. Today, the EU (and therefore Germany, Italy and Spain) and Saudi Arabia are the only members who have integrated cross-border digital identity solutions. Nevertheless, several countries, including Argentina, Australia and Singapore are exploring how to establish such solutions. Australia and Singapore are working on establishing mutually recognised trust frameworks through the

Australia-Singapore Digital Economy Agreement (DEA)[32], and New Zealand, Singapore and Chile through the Digital Economy Partnership Agreement (DEPA)[33] signed in 2020. In Latin America, there is no solution in place but Argentina, Costa Rica and Colombia developed proofs of concept under the framework of the Latin American and Caribbean Council of Civil Registry, Identity and Vital Statistics.

As member of the regional Gulf Cooperation Council (GCC), Saudi Arabia is collaborating with Bahrain, Kuwait, Oman, Qatar, Saudi Arabia, and the United Arab Emirates to integrate the member states' different digital identity systems. As of today, the digital identity system of Bahrain is fully integrated with the Saudi digital identity system and Saudi Arabia is in the process of integrating its system also with the remaining countries. When agreeing to mutual recognition between countries, Saudi Arabia uses legislation and policy mapping to establish the extent to which privacy protection and data security approaches of the other country are consistent with their domestic policies. GCC countries share some mandatory laws or model laws that facilitate this process.

In the EU, as presented throughout this report, the eIDAS regulation and associated implementing regulation provided the regulatory framework and standards necessary to achieve technical and cross-border interoperability between the EU Member States. Italy, Spain and Germany who are all part of the EU, have digital identity systems notified under eIDAS, which allow them to be used in other countries within the EU, and for other EU member digital identities to be used for authentication in order to access domestic services. Although the United Kingdom had previously notified its digital identity solution under eIDAS, following Brexit the country is no longer party to these arrangements. As expressed by the United Kingdom, in order for the country to be able to agree on mutual recognition of digital identity with another country, compliance with the United Kingdom's GDPR and an adequacy determination by assessing the data protection and security approaches of another country would first be necessary.

Cross-border portability is not just relevant between countries but can also cover other administrative and jurisdiction boundaries. Many public services that require proof of identity are provided by local, regional or state governments. In the United States, identities are generated at the State government level and used to create state government level identity credentials. At the federal level, the US government is working to recognise identities from the state and local levels to enable secure digital access to federal services. As with EU Member States that adhere to specific standards and practices in order for their digital identities to be recognised and verified within the union, the work of the United States federal government attempts to address the fragmentation of digital identity systems to simplify the ability for citizens to access services, without establishing a centrally controlled system or database.

[32] https://www.dfat.gov.au/trade/services-and-digital-trade/australia-and-singapore-digital-economy-agreement

[33] https://www.mti.gov.sg/Improving-Trade/Digital-Economy-Agreements/The-Digital-Economy-Partnership-Agreement

Table 3.8. Implemented or plans for cross-border digital identity

	Number of countries where non-citizens can use their domestic digital identity to authenticate themselves for accessing public services	List of countries	Region of recognised digital identities
Germany	8	Belgium, Croatia, Czech Republic, Estonia, Italy, Latvia, Malta, Netherlands	Europe
Italy	23	Portugal, Finland, Croatia, Austria, Denmark, United Kingdom, Luxembourg, Latvia, Slovenia, Netherlands, Slovakia, Czechia, Ireland, Lithuania, Malta, Spain, Estonia, Sweden, Greece, Cyprus, Germany, Belgium, and Norway.	Europe
Saudi Arabia	1	Bahrain	Gulf Cooperation Council
Spain	13	Germany, Italy, Luxembourg, Estonia, Croatia, Belgium, Portugal, Netherlands, Czech Republic, Latvia, Slovakia, Denmark, Lithuania.	Europe
Argentina	Exploratory – not implemented	Colombia, Costa Rica	Latin American and Caribbean Council of Civil Registry, Identity and Vital Statistics
Australia	Exploratory - not implemented	Singapore, New Zealand	South East Asia, Oceania
Singapore	Exploratory - not implemented	Australia, Chile, New Zealand	South East Asia, Oceania

Note: Information is not available for Canada, China, France, India, Indonesia, Japan, Korea, Mexico, South Africa and the United States. Information was also provided by Democratic Republic of Congo, Indonesia and Mexico where digital identity solutions are currently under development.
Source: OECD (2021), "G20 Digital Identity Survey", desk research.

Priorities for future developments

Legislation and policy

As countries work to develop digital identity systems that are fit for the 21st century, governments are considering how to adjust the regulatory framework, policies and identity standards for digital identity. In the United Kingdom, the government is developing digital identity standards to promote an enabling identity market. In February 2021, the government published a prototype of the UK digital identity and attributes Trust Framework, which contains rules on privacy and data protection, fraud management, security, and making sure products and services are inclusive. The trust framework has initially been published as an alpha in order to be tested with services, industries, organisations and potential users. The next version of the trust framework, its beta phase, will be published over the course of 2021. The United Kingdom's government is also preparing to consult on digital identity legislation with proposals for a governing body to own and manage the trust framework to build public and industry confidence in this new market.

Australia and Saudi Arabia are also working on updating legislation related to digital identity. Saudi Arabia is updating the e-transaction law (draft Digital Transactions and Trust Services Law) to add more legal provisions related to digital identities and trust services, and to harmonize with other international laws like e-IDAS and UN model laws. As a complement to new regulatory instruments, Saudi Arabia is also developing a national strategy for digital identity, covering governance model, digital identity and trust services, operating model and service delivery, standards, return on investment and liquidation, and

technical architecture. In Australia, the government is consulting on a proposal for legislation to extend the Trusted Digital Identity Framework (TDIF) beyond federal government agencies to state and territory agencies and the private sector.

Plans for cross-border portability

There are several plans across the surveyed courtiers for improving the way in which digital identity solutions can be used across sectors and borders, which includes taking note of global experiences in the design and delivery of digital identity and explore the potential of mutually recognised trust frameworks. The Government of Australia is looking into opportunities of mutually recognising Trust Frameworks with the governments of Singapore and New Zealand. Australia notes that mutual recognition is a complex challenge that will take several years to complete and the Digital Transformation Agency is using a phased approach to mutual recognition, derived from the European Union's Interoperability Framework and adapted from the World Bank's Digital Identity Practitioners Guide. Singapore is also looking to establish cross border interoperability with other countries, and the government recognises the importance of identification in cross-border transactions, such as visa applications, business registrations, which are onerous and time-consuming, and which could be addressed by having interoperable Digital Identities.

Decentralised identity

Several countries are exploring the possibility of implementing decentralised or self-sovereign identity (SSI) systems. In Europe, the proposed framework for a European Digital Identity by the EU Commission (Proposal for a Regulation amending Regulation (EU) No 910/2014 as regards to establishing a framework for a European Digital Identity (COM(2021) 281 final) on 3 June 2021 is helping to drive this work. Through the framework, European Digital Identity wallets will enable people to choose which aspects of their identity, data and certificates they share with third parties, and to keep track of it. Several Member States have made use of the Recovery and Resilience Facility financial support to public investments and reforms[34] to work on implementing the proposed framework. In Germany, one interdepartmental initiative with the participation of the Federal Chancellery is working to build an SSI-based eID ecosystem and in another, technical solutions are being tested, harmonized and prepared for rollout in four large-scale showcase projects together with citizens, municipalities and SMEs over 2021-2024. Other countries which have plans on pursuing decentralised identity include Singapore and Saudi Arabia.

[34] https://ec.europa.eu/commission/presscorner/detail/en/IP_21_2663

4 Concluding observations

Although G20 members have different priorities and methodologies for the development of digital identity there are five areas in which their experience can be understood as aligning for some overall observations.

Firstly, unlocking the role of digital identity in society is linked to **the availability of opportunities to put digital identity to use**. There is limited value in a digital identity that is not integrated into the day to day life of citizens. As such, there is value in making it as easy as possible for service providers to implement and integrate the national digital identity solution. Moreover, the pursuit of digital identity solutions that can straddle the public and private sectors to offer citizens a seamless route to proving their identity can help digital identity become a ubiquitous habit, rather than an occasional experience.

Secondly, when citizens are given those opportunities to use digital identity they need to be supported by **the quality of the user experience** in doing so. When it comes to someone's experience of the initial enrolment as well as the ongoing experience, the most effective digital identities are transformative in the services they enable, and the experience they offer a citizen.

Thirdly, a crucial part of determining the quality of a user's experience with digital identity, and the opportunities it affords, is **the role of digital identity in the citizen's ownership and visibility of how their data is being used** once authentication has been achieved. Some countries are providing opportunities for citizens to audit the access and use of their data and others are using their digital identity solution as the mechanism by which they surface and secure consents. The architecture of federated models (such as those found in Australia, Italy, the United Kingdom, the United States and to some extent under the provisions of eIDAS within the European Union) avoids creating a single joined-up view of data access for an individual. This reflects a deliberate decision to emphasise individual rights to privacy and ensure there is no scope for overall government oversight into an individual citizens' habits and behaviours.

Fourthly, this question of protecting data and privacy underlines **the critical importance of the governance for digital identity**. This governance helps to ensure effective legal frameworks for supporting a country's approach to digital identity and the associated implications of the exchange and access to data. In addition, digital identity relies on leadership to establish a vision to unlock its full transformational potential as well as the resources (financial, technical and human) to support that vision being made a reality. There is a clear pattern from the experiences of the countries discussed in this paper to look to how a central function handling both strategic leadership and delivery oversight can underpin digital identity solutions and help to work through the challenges associated with exploring compatibility of solutions developed under different jurisdictions

These four points all contribute to outcomes that are citizen focused and built on a foundation for achieving the portability of digital identity: **digital identity is of most value when citizens can authenticate and verify their identity as easily as possible in any given context**. This surfaces the importance of three key tenets in the discussion of digital identity.

1. **It is important that Digital Identity solutions work on a cross-platform basis**: that is, they work when individuals are in front of a desktop computer in their home or accessing services on the move via their mobile phone.
2. **It is important that Digital Identity solutions work on a cross-sectoral basis**: that is, public services can recognise digital identity solutions that can also be used in the private sector. As has

been seen, there are multiple models of digital identity that countries can choose to use and whether public sector identities are recognised for private services, or vice versa, the pursuit of coherent frameworks towards trusted identities are essential for minimising confusing duplication for citizens and increasing the overall trustworthiness of digital identity in society.

3. **It is important that Digital Identity solutions operate effectively on a cross-border basis**. There are many advantages to governments in recognising the validity of digital identities originally provisioned by another country or jurisdiction.

This paper describes the experience of digital identity within the G20 and highlights the different lessons and opportunities found in these varied approaches. Digital identity can be an important enabler for addressing some of the challenges facing the world in the aftermath of COVID-19, not only in the domestic context but across borders too.

The G20 provides a valuable forum to explore greater cross-border cooperation to meet the needs of societies and economies. In the twenty-first century, many of those needs can be traced back to the need for reliable and portable digital identity. Whether it is meeting the needs of diaspora communities looking to simplify their integration into their new homes, or of displaced persons uprooted from theirs and looking for sanctuary and safety elsewhere, or those quarantined and locked down as visitors to countries when a pandemic hit, there are huge potential benefits for unlocking the value of the digital identity individuals carry in their pockets, regardless of the territory in which it was issued.

Reconciling different domestic solutions may seem challenging but the practices collected in this paper show that there are existing patterns for meeting this need. In the European Union, the ambition for its citizens to have a digital identity for use across the Single Market is not based on a single, European identity, but a network of domestic approaches and domestic responsibility for identity data bound together in trust through the eIDAS regulation. On the other side of the world, Australia, New Zealand and Singapore are making progress on their own multi-lateral framework for trusted mutual recognition of digital identity, while Argentina, Costa Rica and Colombia have developed proofs of concept under the framework of the Latin American and Caribbean Council of Civil Registry, Identity and Vital Statistics. Moreover, in federal countries, such as the United States, the approach to digital identity nationally is reliant on a trust framework that recognises identities issued within sub-national jurisdictions. These national and domestic experiences point to an increasing consensus that technical and practical interoperability of digital identity mechanisms is an essential and achievable outcome.

Annex: Collection of digital identity practices

Argentina

1. National context

Argentina is a federal government and SID (*Sistema de Identidad Digital*) is the national solution for digital identity. SID reflects a public sector managed model that can be used for accessing both private and public sector services.

In Argentina, digital identity is available from birth, which means that the total population of the country, which in 2021 was 46.8 million, is eligible for a digital identity.

2. Current national Digital Identity management system

The country model

The digital identity model in Argentina relies on a biometric approach to validating identity using facial recognition and fingerprints based on the government's own identity registration and the information held in the National Registry of People (*Registro Nacional de las Personas*, RENAPER).

There is no distinction between access to public and private sector services uses this solution.

All services can be accessed with physical identity: there is no service that is exclusively accessible through digital identity only.

- The National Registry of People (RENAPER), which answers to the Ministry of Interior, is responsible for the identification of people in Argentina. The Ministry of Interior is the source of funding for digital identity in Argentina.
- The Secretariat of Public Innovation (SIP) from the Chief of Cabinet of Minister´s Office is responsible for the design, proposal and coordination of administrative innovation and technological policies in different areas of government and both the central and decentralised contexts. SIP is also responsible for establishing the strategic direction and proposing regulation in this area, understanding digital government, and collaborating with the provinces and municipalities in their innovation processes.
- The Undersecretariat of Administrative Innovation from the SIP has competencies to implement those initiatives related to document management, procedures, remote processing services and electronic authentication systems for people. Decree 1265/2016 established the Central Electronic Authentication Platform (PAEC) under the management of the Undersecretariat of Administrative Innovation. PAEC allows for remote procedures for natural persons and legal entities, as well as the coordination of interoperability and consolidation of identification systems, to achieve

unambiguous identification and remote digital signature for physical and legal people, in coordination with the competent areas

- The identification standards and technical protocols in Argentina rely on those set by bodies outside the country. For facial recognition Argentina uses the International Civil Aviation Organisation and for fingerprinting they follow the United States' National Institute of Standards and Technology and the Federal Bureau of Investigation.
- RENAPER provides authentication services to the private sector. In order to be able to use identity verification services, private companies must sign a Memorandum of Understanding (MoU) with RENAPER requesting a specific type of service and committing to comply with the Data Protection Law.
- The Argentinian government collaborates with providers of financial services, private security, and private health care as well as travel agencies and data brokers
- In Argentina, the National Identity Document number (*número de DNI*) is used as a single National Identification Number across all services.
- The initial sign-up for SID has to be done in person in order to capture the biometric data.

Technical choices

These biometric elements are sent to the APIs from the National Registry of People (RENAPER, for its Spanish acronym), who processes it and gives back a HIT or NO HIT answer, plus a score regarding the requirements made. It works 24/7.

We work to add digital certificates to expand the identity verification options. In order to obtain and enrol the citizens' biometric data, a government platform manages procedures regarding National Identity Documents (DNI, for its Spanish acronym) and Passports, administrating information from the physical office to the ABIS which manages the biometric elements ensuring unique identities for each citizen.

The different means for authentication used in Argentina are e-signatures and two factor authentication (2FA) that requires access to biometric information whether facial recognition, voice printing, fingerprinting.

Law 25.506 recognises electronic and digital signature. The Secretariat of Public Innovation is the authority responsible for the application of the normative regime which establishes the infrastructure for the digital signature stipulated in the Law. In addition to this, through the Undersecretariat of Administrative Innovation, the Secretariat of Public Innovation is involved in the regulatory framework of the regime related to the legal validity of a document and the digital signature and their addition to the circuit of information of the National Public Service and its paperless archive. Digital signature is used in applications and official systems of the National Public Service. Citizens can freely access digital certificates, and, more precisely, to the digital signature with a token device or to a remote digital signature solution through the Remote Digital Signature Platform (PDRF).

98% of the population that has a digital identity uses the 2FA requiring access to biometric information. With 5 250 000 transactions carried out per month. The biometric elements are collected by RENAPER offices or each province´s civil registers. They are later processed in the AFIS and stored in the backend of RENAPER. The use of these elements is managed by RENAPER.

Portable (cross-platform, cross-sectoral, cross-border) digital identity

- **Cross-platform:** SID is not available through mobile devices.
- **Cross-sectoral:** There is no distinction of use regarding the private or public sector. RENAPER provides authentication services to the private sector. In order to be able to use identity verification services, private companies must sign a Memorandum of Understanding (MoU) with RENAPER requesting a specific type of service and committing to comply with the Data Protection Law. Of all

the possible non-public sector services (private sector and other providers of services) that could be using available digital identity solutions, between 25%-49% are doing so.

- **Cross-border:** No foreign digital identity is recognised in Argentina and SID cannot be used elsewhere. However, proofs of concept have been developed under the framework of the Latin American and Caribbean Council of Civil Registry, Identity and Vital Statistics with Colombia and Costa Rica.

Data visibility and citizen consents

In Argentina, law 17671 provides citizens with the legal right to opt out of the use of a digital identity with all services alternatively being accessible via physical identification.

Digital Identity systems fall within the scope of the Argentine data protection legislation to the extent that they involve personal data processing. Section 2 of Act No. 25.326 defines the term “personal data” as “Information of any kind relating to individuals or legal entities, determined or determinable”. Section 2 of Act No. 25.326 defines the term “data processing” as “Systematic operations and procedures, electronic or not, that allow the collection, conservation, arrangement, storage, modification, relation, evaluation, blocking, destruction, and in general the processing of personal data, as well as its transfer to third parties through communications, consultations, interconnections or transfers”.

The most important regulations that comprise the Argentine data protection framework are as follows:

- Section 43 of the National Constitution[35]
- Act No. 25.326 on Personal Data Protection[36]
- Decree No. 1558/2001[37]
- Act No. 27.483, which approves the ratification of the Convention for the Protection of Individuals regarding Automatic Processing of Personal Data of the Council of Europe (better known as "Convention 108")[38]

The National Direction of Personal Data Protection, operating within Agency for Access to Public Information (AAIP) is the Argentinian authority that monitors and oversees the impact of Digital Identity on individual privacy and freedoms. The AAIP is a public body that acts as oversight authority at a national level for both Access to Information and Data Protection laws. It was created by Act No. 27.275 on Access to Public Information.

Among other functions and powers granted to the AAIP in order to control the compliance with Act No. 25.326, the Agency may request information from public and private entities regarding their data processing operations, impose administrative sanctions that may be applicable for violation of the provisions of Act No. 25.362, or request judicial authorization to access establishments, equipment, or data processing programs in order to verify violations of compliance with this law. Article 24 of Law 27275 establishes that the AAIP has its own annual budget, while Article 25 establishes that the agency will have the technical and administrative staff established by the general budget law of the national administration.

The Argentine data protection framework does not prohibit commercialization of data but sets out a series of mandatory rules that must be respected by data controllers/processors:

[35] http://servicios.infoleg.gob.ar/infolegInternet/anexos/0-4999/804/norma.htm

[36] http://servicios.infoleg.gob.ar/infolegInternet/anexos/60000-64999/64790/texact.htm

[37] http://servicios.infoleg.gob.ar/infolegInternet/anexos/70000-74999/70368/texact.htm

[38] http://servicios.infoleg.gob.ar/infolegInternet/anexos/315000-319999/318245/norma.htm

- Pursuant to section 5 of Act No. 25.326, data controllers must request the data subject's free, unambiguous, and informed consent prior to processing his/her personal data.
- Section 11 of Act No. 25.326 establishes that controllers must require the data subject's consent prior to transferring his/her data to another data controller/processor.
- Section 4 of Law No. 25,326 sets forth rules on purpose limitation, proportionality, data minimization and data retention.
- Section 6 of Law No. 25.326 establishes rules on transparency and information that must be provided to data subjects whenever his/her data is processed.
- Data subjects have the right to request access, rectification, or erasure of their data from data controllers.
- They also have the right to file a complaint before the AAIP or the competent Court (Section 43 of the National Constitution and sections 14, 15 and 16 of Law No. 25,326).
- In technical terms, the consent is between private parties, the National Registry of people only exposes a backend that returns only HIT or no HIT. Access to the APIs is protected with signed tokens and centralized user administration by RENAPER.

Data controllers and processors, whether private or public, have an obligation to adopt appropriate security measures in order to ensure security and confidentiality of the personal information they process (sections 9 and 10 of Act No. 25,326). Furthermore, the AAIP issued Resolution No. 47/2018[39], which lists a series of recommendations that data controllers/processors should consider in order to comply with their security and confidentiality obligations.

In technical terms, the data entered with the user's consent, that is, the image of their face or the images of their fingerprints, are taken from the API hosted in the cloud to the RENAPER backend where, once the identity verification has been carried out, they are eliminated, and only HIT or NO HIT is returned.

Argentinian citizens are not proactively informed by authorities about any processing of their personally identifiable data. However, users of SID can access and see what attributes or data are being shared/re-used, and with/by whom through the provisions of Article 11 of Law 25326 in the expectation their consent has been sought (and can be revoked):

The personal data object of treatment can only be transferred for the fulfilment of the purposes directly related to the legitimate interest of the transferor and the assignee and with the prior consent of the owner of the data, who must be informed about the purpose of the transfer and identify the transferee or the elements that allow it to do so. The consent for the assignment is revocable.

Civil society organisations are able to monitor the process by which a person's identifiable data is shared and reused:

- Law No. 17.671 regulates citizen identification procedures.
- Sections 5 and 7 of Law No. 25.326 establish the legal basis under which data controllers may process personal data. Among other legal basis, processing shall be lawful in the following scenarios:
  - When the data subject has given his consent to the processing of his/her personal data.
  - When processing is necessary for the performance of a contract.
  - When processing is necessary for compliance with a legal obligation to which the controller is subject.
  - When processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller.

[39] http://servicios.infoleg.gob.ar/infolegInternet/anexos/310000-314999/312662/norma.htm

- Regarding proportionality, section 4 of Law No. 25.326 requires controllers to process only data that is adequate, relevant, and not excessive in relation to the purposes for which the data was obtained. It also establishes an obligation to destroy data when it is no longer necessary or relevant to the purposes for which it was collected.

3. Uptake and adoption of Digital Identity

In December 2019, prior to the COVID-19 pandemic outbreak, the number of individuals with a digital identity was 44 362 630. The percentage of the eligible population that had a digital identity was therefore 94.7%. In April 2021, a year after the first wave of the pandemic, the total population with an active access to a digital identity was 44 503 167, meaning the share of eligible population with a digital identity had increased marginally to 95%.

This reflects that a biometric approach to digital identity expects to incorporate 100% of society through their enrolment at birth.

In Argentina it is not mandatory for public sector organisations to use SID for service user authentication and verification. Out of all public sector services where it would be necessary to authenticate users, 75-99% were using it in 2021. In the private sector this figure is 25%-49%.

Both public and private sector service teams which rely on SID are able to access technical support both at the point of integration and on an ongoing basis with support provided by a 24/7 help desk.

The work regarding the digitalization of identity, that began in 2009, allowed, during the beginning of the pandemic, the remote access to financial servicesof millions of citizens that couldn´t circulate due to the restrictions and needed the state´s financial help.

On the other hand, remote authentication and processing solutions were already implemented, and we worked to support the growth of authentication transactions on the Central Electronic Authentication Platform and to connect new client systems to the Platform. In 2020, the Platform and the service AUTENTICAR were integrated with 44 client applications, making a total of 123 the systems which make use of electronic authentication services.

4. Ongoing and future Digital Identity reforms

The Argentinian government is currently working on a project to implement an electronic DNI to store a digital identity certificate and an individual’s digital signature.

Australia

1. National context

Australia is a federal government and the national solution for digital identity, operating under the brand myGov, reflects a federated model. Users are able to choose their preferred identity provider from a choice of public and private sector suppliers to prove their identity and allow them to access Australian public services.

In Australia, all individuals above 15 years old can request a digital identity. The total population of the country in 2021 was 25.7 million, with the total population eligible for a digital identity (based on age) 19.9 million, or 77% of the total population.

2. Current national Digital Identity management system

The country model

Australia's model for providing digital identity is not based on public sector identity materials through a public sector governed and delivered standalone digital identity solution. Instead, the myGov model in Australia consists of a federated approach where *private sector and public sector managed digital identity providers offer their services to users who wish to have their identity verified. Currently, users can only access government services provided at both a federal and territorial level.*

- The strategic direction of and vision for the Australian Government's Digital Identity system is steered by the Digital Transformation Agency in collaboration with Australian Government delivery partners and other system stakeholders. Policy direction is set by the Australian Government Minister for Employment, Workforce, Skills, Small and Family Business and Minister for Government Services. The delivery of the Australia Government's Digital Identity system is overseen by the Digital Transformation Agency in collaboration with Australian Government delivery partners.
- The Australian Government's Digital Identity system is currently fully funded by the government, with a view to implementing a charging framework to address the long term sustainability of the system.
- The Australian Government's National Identity Proofing Guidelines (NIPGs) provide a robust, yet flexible risk based approach and set of guidelines to identity proofing and conducting identification, aligned with international best-practice standards. The NIPGs define four Identity Proofing (IP) levels, which can be applied through a risk-based assessment across individual interactions and identity requirements. The Trusted Digital Identity Framework (TDIF) also provides a framework for entities conducting roles as part of the Australian Government's Digital Identity system, which itself references international standards. This framework aligns to the NIPGs where appropriate.
- The Trusted Digital Identity Framework (TDIF) is an accreditation framework for the Australian Government Digital Identity system. It sets out the requirements that applicants need to meet to achieve accreditation. This includes identity providers and their ability to meet the identification requirements under the TDIF. Identity providers must be accredited under the TDIF to participate in the Australian Digital Identity system. Once accredited, providers need to continually demonstrate they meet their TDIF obligations by undergoing annual assessments.
- The Australian government collaborates with non-public sector actors around digital identity, including mobile operators, IdP companies, bank and financial services, academia, and software companies. Non-public sector services are able to participate in the Australian Government Digital Identity system under the TDIF. They are also engaged in development of the TDIF and Digital Identity system.
- People can obtain a Digital Identity in the Australian Government's Digital Identity system through a simple, streamlined online-only process using the Australian Government's identity provider, myGovID. The three-step process requires people to have a smart device and an email address, and be 15 years or older:
    1. Download the myGovID app (available on the Apple App Store and Google Play)
    2. Enter their details, including full name, date of birth and email address. After entering these details people have a Basic identity strength, with access to limited government online services.
    3. Verify their Australian identity documents, such as a passport, birth certificate, driver's license or visa, which will be verified using the Australia Government's Document Verification System. After verifying their identity documents people have a Standard identity strength which allows access to all participating government online services.

- The Australian Government's Digital Identity system is currently developing the capability for biometric verification to support a stronger identity strength. There is no National Identification Number used across all services, nor other mechanisms for connecting records between organisations.

Technical choices

The Australian Government's Digital Identity system uses two-factor authentication that confirms access to a mobile device through the myGovID mobile application. The system is developing the capability for biometric verification to support a stronger identity strength.

Portable (cross-platform, cross-sectoral, cross-border) digital identity

- **Cross-platform:** The Australian Government's Digital Identity system is available through Android and iOS based mobile devices via the myGovID app. Requests that require confirmation via myGovID are initiated within a browser and then secured using the app as a second factor for authentication
- **Cross-sectoral**: In Australia myGov currently only supports public sector services
- **Cross-border:** Australia is paying attention to global experiences in the design and delivery of digital identity and are exploring opportunities of mutually recognising Trust Frameworks with the governments of Singapore and New Zealand. Australia also leads the Digital Government Exchange (DGX) Digital Identity working group. The Digital Transformation Agency (DTA) has participated in ID4Good (Cybersecurity considerations and improving citizen experience with Digital identity) and the World Economic Forum (contributing to the paper on Identity in a Digital World: A new chapter in the social contract). We recognise that mutual recognition is a complex challenge that will take several years to complete. The Australian Government's Digital Transformation Agency is using a phased approach to mutual recognition, derived from the European Union's Interoperability Framework and adapted from the World Bank's Digital Identity Practitioners Guide.

Data visibility and citizen consents

The use of Digital Identity in Australia is voluntary for citizens, which also seeks to be strengthened by the proposed Trusted Digital Identity Legislation in development.

There are multiple layers of privacy related rules applying to data entering the Australian Government's Digital Identity system, including:

- Commonwealth Privacy Act, the key federal legislation applying to data and privacy. Privacy protections are contained in 13 Australian Privacy Principles APPs), principles-based laws which can be interpreted and applied to the context of their organisations. The responsible agency is currently undertaking a review of the Act, so the rules in the Act could change in the future.
- State based legislation, which governs how state entities handle personal information. Most state-based legislations are similar to the Commonwealth Privacy Act and must be to be recognised for accreditation purposes under the TDIF.
- The TDIF was developed to supplement existing Australian law and ensure that personal data entering the Australian Government Digital Identity system is subject to stringent privacy protections.
- The TDIF contains a number of privacy specific rules, including rules which require accredited participants to conduct privacy impact assessment for high risk changes to their system, have

privacy officers and privacy champions, only use behavioural information in certain ways, and seek explicit and informed consent before sharing an individual's attributes with a relying party.

The Australian Government is currently drafting new legislation to govern the Australian Government Digital Identity system. This legislation will contain a number of new, strong and in some cases novel privacy protections which will add new protections to data entering the system. The policy for these protections is still being consulted on, but will likely include areas like biometrics, profiling, and limits on the creation of unique identifiers.

Accreditation under the Trusted Digital Identity Framework (TDIF) is open to the private sector. All organisations that are accredited as providers of Digital Identity and with roles under the TDIF in the Australian Government's Digital Identity System must comply with the TDIF's stringent privacy, fraud, and protective security requirements. To become a TDIF accredited provider, applicants are required to demonstrate how their Digital Identity service meets requirements for accessibility and usability, privacy protection, security and fraud control, risk management, technical integrity and more. This includes the need for:

- an independent privacy impact assessment
- an independent security assessment
- ICT penetration test
- Organisational policies and practices that demonstrate alignment with the Australian Government Protective Security Policy Framework, the Information Security Manual, the Australian Privacy Principles and the Privacy Code.

The requirements defined in the framework build on the baseline of the Australian Cyber Security Centre's Essential Eight cyber security mitigations. They also meet the requirements of organisations under the Privacy Act 1988 (Cth). Once accredited, providers need to continually demonstrate they meet their TDIF obligations by undergoing annual assessments.

Users of the Australian Government's Digital Identity system can access and view the attributes and data that are being shared with participants in the system through the use of their Digital Identity, they are also able to control their consents for the attributes and data that are being shared with participants in the system. The TDIF has requirements that disallow accredited providers (including private sector accredited providers) from disclosing a user's data without their consent. It also has requirements that prevent organisations from using personal information for direct marketing purposes. These safeguards will be further strengthened in the Digital Identity legislation.

The Australian Government's Digital Identity system maintained strong security controls and privacy safeguards to protect user privacy throughout the COVID-19 pandemic. There have been no instances identified where the system has been unable to protect user privacy.

3. Uptake and adoption of Digital Identity

In Australia, it is not mandatory for the public sector to use the available digital identity solutions for service user authentication and verification. There are no available figures on the proportion of public services that require user authentication that use the available digital identity solution. Non-government actors cannot currently integrate the Australian Government Digital Identity system into the services they provide to the public.

In December 2019, prior to the COVID-19 pandemic outbreak, the number of individuals with a digital identity was 128 000. The percentage of the eligible population that had a digital identity was therefore 0.64%. In April 2021, a year after the first wave of the pandemic, the total population with an active access to a digital identity was 2.3 million, meaning the share of eligible population with a digital identity had increased roughly 11 percentage points to 11.35%.

The Australian Government's Digital Identity system provides a way for people to log in to myGov, the primary portal for individuals to access Australian Government digital services. myGov also provides access to people's COVID-19 Vaccination Certificates, which supports Australia's recovery from the COVID-19 pandemic and may become essential for reopening international borders. Strong authentication and verification methods like the Digital Identity system guard against fraud and ensures the person applying for the certificate is who they say they are. In the future, this could feasibly enable a strong, internationally recognised and interoperable COVID-19 Vaccination Certificate to support international travel through integration of a person's Digital Identity and digital wallet.

The Digital Identity system was used by most Australian businesses to access services and support during the COVID-19 pandemic. It was also integrated with the Australian Government's primary individual portal, myGov, to support individuals to access government services and support. The Australian Government has also recognised that Digital Identity can also provide essential support in the case of natural disasters, demonstrated during the 2019-2020 Australian bushfires. Once a Digital Identity has been created, it removes the need to find identity documents such as birth certificates, passports which may have been lost, allowing for faster access to government services and relief payments.

4. Ongoing and future Digital Identity reforms

The Australian government is working on rolling out a whole-of-economy Digital Identity system to include state, territory and local government, as well as the private sector. To this end, the Australian Government is currently developing legislation to:

- allow for independent oversight of the system, by formalising the powers and governance arrangements of the independent Oversight Authority
- enable the system to expand to state, territory and local governments and the private sector
- ensure privacy protections and consumer safeguards to build trust in the system
- Provide a legally enforceable set of rules that set the standards for participating in the Digital Identity system, including for accreditation.
- Allow for entities to be accredited for their activities whether they are on or not on the system.

The biggest lesson that the Australian government has learned throughout its digital identity reforms is to develop clear policy positions and trust frameworks to support the development and build of the system, and to develop these using already established best practice and standards where possible to optimise the opportunity for interoperability. Moreover, the importance of focusing on the benefits to the end users, the impacts of improved access to services, and the increase in productivity and fraud management to help build the case for change.

Brazil

1. National context

The current national digital identity of Brazil is provided by the GOV.BR digital identity platform provided by the federal government. The digital identity solution makes use of biometric technology.

In Brazil, individuals can have a digital identity from the age of 16. In 2021, the total population of Brazil was 213 million, with 170 million, or 80% of the total population, being eligible for a digital identity.

2. Current national Digital Identity management system

The country model

Brazil has a shared digital identity management system model, where the management of the digital identity system is shared jointly by public and private sectors for accessing both private and public sector services.

- The Ministry of Economy steers the strategic vision for and direction of digital identity while the Special Secretariat for Modernization of the State in General-Secretariat of the Presidency oversees its delivery.
- The digital identity system is funded by the federal government budget.
- In terms of standards for digital identity, the Steering Committee of the National Civil Identification have passed a number of legislative resolutions providing recommendations concerning biometric standards and the National Civil ID registry including:
  - Collect fingerprints of all hand fingers;
  - ANSI-INCITS 378/2004: common fingerprints minutiae for data exchange;
  - ICAO 9303: standard documentation used by the International Civil Aviation Organization, when it comes to facial biometrics;
  - ISO/IEC FCD 19794: setting common biometric exchange formats framework, such as ISO/UEC FCD 19794-2 and ISO/UEC FCD 19794-4 (common fingerprints formats frameworks - *padrões de impressão digital*) ISO/IEC FCD 19794-5 (common facial image formats framework - *padrões de imagem facial*);
  - ANSIINIST ITL 1-2000 e ANSI/NIST ITL 2-2008 - common data standards format framework for digital data exchange;
  - WSQ *Versão* 3.1: common compression and image storage algorithm of fingerprints;
  - CBEFF (common biometric exchange formats framework) : *padrão de intercâmbio de dados biométricos.*
- The Brazilian government collaborates with banks and financial services, as well as academia around digital identity. Brazil's digital identity system is integrated with the authentication platforms of large banks.
- The development of a national digital identity system in Brazil has been supported by Law nº 13.444/2017 that introduced the National Civil Registration - *Identificação Civil Nacional* - ICN, which aims at providing proof of legal identity to Brazilians when accessing public services as well as in their relations with the private sector. The above-mentioned legislation also created the Steering Committee of the National Civil Identification - *Comitê Gestor da Identificação Civil Nacional* -, which is composed by members of the three branches of the Public Administration. The Superior Electoral Court and the Federal Executive branch take turns as the head of the Committee every two years. The Committee's decisions require a majority of two-thirds to be put into force. The Committee can recommend biometric standards, as well as participate in the formation rule for the National ID number. It can also set guidelines for the administration of the National Civil Identification Fund - *Fundo da Identificação Civil Nacional* (FICN) and for resources management. Moreover, the Committee provides guidance to the implementation of interoperability between the electronic systems of the Federal Executive Branch and the Electoral Justice.
- Brazil does not have a national identification number across all services. Instead, the number of CPF (a federal tax ID), managed by the Special Department of Federal Revenue of Brazil is used for connecting records between organisations or services. The tax number - *Cadastro de Pessoas Físicas* (CPF) – forms the basis of the number of the National Civil Identification - *Identificação Civil Nacional* (ICN) -, for daily and "public use". There is an internally restricted number for the

ICN in order to assure uniqueness. This restricted number will be linked to an individual biometric registration and a single tax number as well

- Citizens can use different methods to complete the on boarding online in order to get a digital identity. Citizens can complete the on boarding process through the website address acesso.gov.br and have the support using the app (Meu gov.br) which is available at Google play and Apple Store. All of them require the citizen to have their CPF, which is a sufficient condition to access any public service in Brazil. The steps to obtain a digital identity are:
  - **Bronze Category - *Classificação Bronze***
    - Based on Knowledge-based Authentication (KBA), citizens must answer questions related to personal data, as well as their labour and pension records.
  - **Silver Category - *Classificação Prata***
    - Based on banking authentication, bank customers can, by means of bank digital identity login, identify themselves at GOV.BR Identity platform
    - Based on facial biometrics saved in the driver 's license database, using mobile phone cameras.
  - **Gold Category - *Classificação Ouro***
    - Based on facial biometrics stored in the National Civil Identification (ICN) dataset, using the mobile phone cameras. Currently, the database holds biometric data for 118 million Brazilians.

Technical choices

In Brazil, the means for authentication used via the digital identity include digital certificate file, username and password, and two-factor authentication that requires access to a mobile device. Facial biometrics are also gathered and used.

- Digital certificates are considered especially valuable for the private sector organisations who access government services from the Brazilian Federal Revenue Office. Per month, 300 000 authentications/verification are issued via digital certificates by any available digital identity solution.
- Username and password are currently providing access to more than a thousand digital public services. Per month, 140 million authentication/verifications are issued by any available digital identity solution.
- Per month, 350 000 authentication/verifications are issued using two-factor authentication that confirms access to a mobile device.
- There is no figure available on the number of authentications/verifications issued that requires access to biometric information.

Portable (cross-platform, cross-sectoral, cross-border) digital identity

- **Cross-platform:** The national digital identity solution in Brazil can be accessed from mobile devices which allow for cross-platform portability.
- **Cross-sectoral:** The available digital identity solutions in Brazil can be used both by businesses and citizens to access public services. The digital identity solution for GOV.br is integrated with the bank authentication platform, which implies there is cross-sectoral portability for the bank authentication platform solution. The public sector managed digital identity solution cannot be used for accessing non-government services.

- **Cross-border:** Digital identities from other countries are currently not recognised for authentication and verification in Brazil, and neither is the digital identity of Brazil recognised by other countries for user authentication and verification.

Data visibility and citizen consents

In Brazil, citizens have a legal right to opt out of the use of a digital identity.

Brazil's General Data Protection Law (LGPD) is the law which provides regulations for the processing of personal data either by individuals or by organisations (government or private sector).

The Law creates the National Council for the Protection of Personal Data and Privacy, which will be composed of 23 representatives from the government, parliament, judiciary, productive sectors and civil society. This council is to propose strategic guidelines, preparing annual evaluation reports, suggesting actions to be taken, preparing studies and holding debates and public hearings on the protection of personal data and privacy.

The National Data Protection Authority (ANPD) is part of the Brazilian federal government and linked to the Presidency of Brazil. Although the office of Presidency of Brazil is responsible for the budgets, from a technical and subject matter perspective, ANPD is an independent entity that has competences related to evaluate and address data protection issues. This legal nature is transitory and ANPD may be transformed into an independent federal public administration entity within two years from the date of entry into force of the ANPD regimental structure. The mandate of ANPD includes:

- Exclusively oversee and impose administrative sanctions when LGPD is violated;
- The promotion of data protection and privacy within the Brazilian society;
- Request information regarding the processing of personal data from data processors and controllers;
- Promote cooperation with DPAs from other countries;
- Interpret LGPD

3. Uptake and adoption of Digital Identity

In Brazil, it is mandatory for public sector organisations to use available digital identity solutions for service user authentication and verification. The budget and technical development for digital identity are centralized within The Secretariat of Digital Government of the Ministry of Economy (SGD), which offers a technical team to support public agencies in implementing the digital identity solutions. As of today, 50%-74% of public services where it is necessary to authenticate users are using the available digital identity solutions for service user authentication/verification. On average, individuals use the available digital identity solution to access any public service fifteen times per year.

In December 2019, prior to the COVID-19 pandemic outbreak, the number of individuals with a digital identity was 45 million. The percentage of the eligible population that had a digital identity was therefore 26%. In April 2021, a year after the first wave of the pandemic, the total population with an active digital identity was 97 million, meaning digital identity adoption had increased by 116% to 57%. This figure has gone on to increase to 105 million by June 2021.

- The pandemic saw increased demand not only for digital identity but also access to GOV.BR, the government website with an increase from 54 million in March 2020 to 140 million in May 2021, equivalent to a 159% growth.
- Digital identity is required for accessing a list of more than 3 thousand digital public services through GOV.BR, which is the main reason for visiting the webpage. Some of the digital public services are provided by the Federal government, while others are delivered at the local level - municipalities

and states. Throughout the pandemic the number of services connected to the platform have more than doubled.

- Proof-of-life is one example of a digital service available at GOV.BR Portal. More than 7 million pensioners and retirees that received social security benefits can now update their status and prove they are alive and still eligible for the benefit using mobile and facial recognition technology – this has contributed to public trust and has enhanced the public's acceptance of digitalisation. It has also prevented citizens from going to government venues in order to access the service, avoiding unnecessary social contact during the pandemic.
- The delivery of cash benefits from the government online was one of the services that benefitted the most from digital identity use during the pandemic. This include access to an emergency program for maintaining jobs and income, and social benefits paid by the Social Security National Institute to pensioners and retirees who needed to prove they are alive in order to maintain benefits. In terms of protecting user privacy, digital services that use identifiable data from the digital identity solution provided by the federal government are subject, by default, to information security and privacy protection standards that also helped mitigate risks of data misuse during the pandemic. The unified digital identity solution is already used today in 39% of the digital services of the federal government and over 3.000 digital services in states and municipalities.
- The most important lessons from the use of digital identity during the COVID-19 crisis includes understanding that the use and adoption of a digital identity solution by the population is related to user experience - efforts made to understand user needs, their difficulties and barriers to use, and develop rapid and constant improvements. If user experience is not considered, the users will use shortcuts to pass by the problem which may increase security risks.
- Furthermore, Brazil finds it important to aggregate the existing digital identity solutions to the digital identity platform as an on boarding strategy. In Brazil, it was critical to allow for the use of the existing, secure digital identity solutions already for the financial ecosystem, government official biometrics information, and digital certificate ecosystem in order to facilitate on boarding and promote adoption.

4. Ongoing and future Digital Identity reforms

In recent years, an important set of laws have been put in force in Brazil aiming at fostering the use of digital identity:

- Law 13444/2017, which, introduced the National Civil Identification - ICN. The ICN aims at providing proof of legal identity to Brazilians when they access public services as well as when interacting with the private sector
- Law 14063/2020: Provides for the use of electronic signatures in citizen-government interactions. It is regulated by Decree 10543/2020, which sets the requirements for electronic signatures. Digital identity enables the use of electronic signature.
- Law 14129: Sets principles, rules and instruments for Digital Government. It also states that the tax number is both sufficient as a proof of legal identity for citizens and provides access to other identification documents.

In terms of the most valuable lessons learned through the reforms for the Brazilian government reports "one citizen, one identity and authentication solution for all digital government services". By offering a single cross-platform identity centrally that meets the diverse security and multi-level authentication needs of all digital services, it will result in rapid growth in population adoption. Aggregating the existing solutions in a single platform that gives citizens the feeling of a single cohesive solution is the most appropriate strategy to evolve in the implementation of the solution according to Brazil.

Democratic Republic of Congo

There is currently no national digital identity management system in place in the Democratic Republic of Congo. The existing identification system and related standards are based on the electoral card, which is funded by the Electoral Commission. The Digital Ministry is responsible for setting a strategic vision for digital identity in the country. The Democratic Republic of Congo does not have a legislation in place to protect a person's data connected to the use of a Digital Identity system.

European Union

The European Union provides legislation concerning the functioning of digital identity in all EU Member States and EEA countries. The electronic IDentification, Authentication and trust Services (eIDAS) regulation entered into force in 2014 and oversees electronic identification and trust services for electronic transactions in the European Union's internal market. It regulates electronic signatures, electronic transactions, involved bodies, and their embedding processes to provide a safe way for users to conduct business online like electronic funds transfer or transactions with public services. eIDAS ensures mutual recognition of the eID for authentication among member states in order to achieve the goal of the Digital Single Market. Building on the lessons and experiences of this regulation, the European Commission put forward proposals on 3 June 2021 for a European Digital Identity framework.

In addition to EU level efforts on digital identity, the General Data Protection Regulation (GDPR) provides a cross-European model for data protection and individual consents that are highly relevant in the digital identity conversation and cited by the other European Union member countries in their responses. Furthermore, GDPR has provided an international model with other countries seeking to ensure equivalency with their domestic models in this area.

Germany

1. National context

The current national digital identity of Germany is the eID infrastructure provided by the federal government. The identity solution is provided through a chip which is included in three different types of cards: the German citizen identity card, the electronic residence permit for non-citizens of the EU/EEA area, and the eID card for citizens within the EU or EEA area.

In Germany, individuals aged 16 or above can have the eID. Germany’s total population in 2021 was 83.2 million, and the total eligible population for eID based on age was therefore 62.3 million, or 75% of the total population.

2. Current national Digital Identity management system

The country model

Germany’s model for providing digital identity is sector specific with reusable public digital identity. This means that there are private sector managed digital identity solutions for accessing only private sector services, and public sector managed identity solutions for accessing both public and private sector services.

- The German Federal Ministry of the Interior, Building and Community is responsible for identity management as well as passport and ID systems in Germany and the project Digital Identities of the Federal Government. The Federal Office for Information Security (BSI) carries out the

certification in accordance with the Technical Directive TR-03128-2 of the BSI, which identification service providers must comply with in accordance with Section 21 b of the Act on Identity Cards and Electronic Identification.

- The issuing authority for authorisation certificates (VfB) in the Federal Office of Administration (BVA) grants service providers the state authorisation to read out the identification data from the national online ID when fulfilling the requirements. On behalf of the Federal Ministry of the Interior, Building and Community, the Bundesdruckerei GmbH produces the three online identifiers, which are equipped with the state and certified according to the eIDAS regulation at the highest level of trust. The Bundesdruckerei GmbH is partly state-financed GmbH under the supervision of the Federal Ministry of Finance as investment leader.
- The issuance of the German identity card, the electronic residence permit and the eID card for EU and EEA citizens are charged with fees, which are partially received by Bundesdruckerei GmbH. In addition, there are other private sector identity providers not notified under the eIDAS regulation, which finance themselves privately.
- The EU's eIDAS regulation is implemented in Germany's administration. The requirements for levels of assurance arising from the eIDAS regulation are specified more precisely in Germany by the technical directive of the Federal Office for Information Security (BSI), BSI-TR03107. There are three levels of assurance: high, medium, and normal for identification with administrative services. Identification for private sector offers is partly regulated by domestic laws, such as the Telecommunications Act (TKG) and the Money Laundering Act (GWG).
- The Federal Office for Information Security (BSI) is responsible for the certification of eID products (eID servers, eID clients) and eID applications based on the corresponding technical guidelines (TR) of the BSI. The certification of their eID products and eID applications according to the national BSI-TR is open to German and international companies as well as state institutions.
- As part of the Digital Identities project, the Federal Government is currently working with private sector actors to design an open identity ecosystem based on an SSI wallet. As part of the Digital Identities project, the Federal Government is working with companies from the mobility, banking, hotel, e-commerce and telecommunications sectors. As the future Smart-eID may be be used alongside an eSIM, mobile network operator will increasingly be important as providers of that eSIM.
- In Germany there is currently no single national identification number used across services nor a mechanism connecting records between different organisations or services. The identification number is instead provided and used after a successful identification (e.g. in a user account based on the eID function) to clearly assign data to a natural person in an administrative process. The identification number itself is therefore not treated as an electronic proof of identity. In the future, a so-called identification number will be introduced.
- There is currently no online-only process for users to obtain an eID in Germany. In order to obtain the online ID function, a personal application for one of the three identity cards – the German identity card, the electronic residence permit and the eID card for citizens of the EU and the EEA – is necessary with the respective competent authority. This requires certain evidence and identification by the public authority on the basis of a national identity card. After production of the ID card and before picking up the ID card in the local authority, the applicant receives a PIN letter. This provides important information for the activation and blocking of the online ID function. After picking up the ID card and setting the self-selected, six-digit PIN for the online ID function, the person can use their digital identity. As a response to lessons learnt during the COVID-19 pandemic and the limitations on activating identities, the Federal Government will implement a partial digital process for the subsequent activation of the online ID function as well as for the subsequent online application for a new PIN.

- The eID infrastructure for the online ID function is provided by the federal government. For the electronic proof of identity, the online ID function is provided in a chip. The chip can be read by the service providers for which the electronic identity verification is required, if the service provider (the authority or company) has been granted the State's authorisation. The service provider uses an eID reader connected to the web application.

Technical choices

The German digital identity is accessed through a chip on a smartcard using a card reader. The service provider needs software or an eID client in order to establish the connection between the eID server and the chip card. Users install an eID client on their smartphone or computer which establishes the end-to-end encrypted internet connection between the chip card and the eID server via NFC-enabled smartphones or a card reader.

Bundesdruckerei GmbH supports federal authorities that want to establish their own eID infrastructure for electronic identification with the online ID function, by providing a central eID service, the required authorisation certificates and SSL/TLS certificates as well as technical integration into existing IT systems. eID-service providers support the establishment of their own eID infrastructure and identification service providers take over identification for the Authority as a service. Authorities wishing to connect their services to the user accounts of the Federal Government and the federal states receive support from the competent authorities of the Federal Government (BMI, DV 3) and the 16 federal states.

Portable (cross-platform, cross-sectoral, cross-border) digital identity

- **Cross-platform:** Since 2017 it has been possible for the three German identity cards (the identity card, electronic residence permit or eID card for EU citizens) to operate with mobile devices that are Near-Field Communication (NFC) compatible. The Digital Identities project is currently developing a replacement solution that will work without creating the ID card. In the future, Smart-eID will store the identity data from the smart card in a security element or in an eSIM on your smartphone. The Smart-eID can then be used for identification on the Internet without using the ID card. In future, the Smart-eID can also be used in conjunction with an eSIM. Mobile network operators will increasingly be important in providing the eSIM.
- **Cross-sectoral:** It is possible for non-public organisations, including the private sector, to develop and offer services that use the national online ID.
- **Cross-border:** Pursuant to Regulation (EU) No 910/2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC, or eIDAS regulation, notified eIDs of the European Member States are accepted in Germany. Germany implements the eIDAS regulation. However, not all federal levels are at the same level in implementation. The following list applies to the eIDAS compliant national user account „Nutzerkonto Bund": Belgium, Croatia, Czech Republic, Estonia, Italy, Latvia, Malta, Netherlands, Portugal, Slovakia and Spain. The EU's eIDAS regulation is implemented in Germany's administration. The requirements for levels of assurance arising from the eIDAS regulation are specified more precisely in Germany by the technical directive of the Federal Office for Information Security (BSI), BSI-TR03107. There are three levels of assurance: high, medium, and normal for identification with administrative services.

Data visibility and citizen consents

In Germany, citizens have a legal right to opt out of the use of a digital identity.

When using the online ID function, after the connection between the ID card and the smartphone or the card reader has been established, the user receives information about which provider requests the data and what data is specifically involved.

Before transferring data from the digital identity, the data is displayed to the user, and it is free to the user to decide about the transfer of the data. He or she can also refuse to do so. The use of the state eID function is free of charge for users and service providers. The issuing authority for authorisation certificates (VfB) in the Federal Office of Administration (BVA) grants service providers the state authorisation to read out the identification data from the national online ID when fulfilling the requirements.

The applicable data protection requirements must be complied with, including GDPR and the Federal Data Protection Act. In addition, the user must agree to the transmission of data by entering the self-selected, six-digit PIN. If the user does not enter the PIN, the data will not be transmitted. If the data has been transmitted after PIN input, the transaction cannot be revoked.

3. Uptake and adoption of Digital Identity

In December 2019, prior to the COVID-19 pandemic outbreak, the number of individuals with a digital identity in Germany was 30.3 million. The percentage of the eligible population that had a digital identity was therefore 49%. In April 2021, a year after the first wave of the pandemic, the total population with an active access to a digital identity was 38.3 million, meaning digital identity adoption had increased 26% to 61%. On average individuals use a digital identity solution to access or consume any public sector service 3.2 times per year.

- In Germany, as per § 2 (3) of the EGovernment Act of the Federal Government (EGovG), it is mandatory for all federal authorities to offer an electronic proof of identity in administrative proceedings in which they have to establish the identity of a person on the basis of a legal act or for other reasons. This obligation applies to the public administration activities of the federal authorities, including federal direct corporations, institutions and foundations under public law. According to § 3a of the E-Government Act, the online ID function of the ID card in conjunction with an electronic form, is permitted to replace the written form in federal law.
- In Germany, authorities at all federal levels can entrust eID service providers to support them in setting up their own eID infrastructure, or to entrust identification service providers with the identification of customers. However, it is easier for them to adopt the user accounts offered by the Federal Government and the federal states on their administrative portals. On the Internet portal www.personalausweisportal.de, the Federal Ministry of the Interior, Building and Community provides information for authorities that describe how the online identification function can be integrated into processes. This also includes technical information as well as contact details of eID service providers and identification service providers.
- During the COVID-19 crisis the federal government was able to quickly provide administrative services using digital identity. One example is the financial aid for companies (immediate aid, Corona bridging aids), which could be applied for on a platform provided by the federal government with the use of the citizens' online ID. In this way, companies could also apply for and receive financial assistance during the lockdown periods. In Germany, the COVID-19-related restrictions have led temporarily to a complete closure of citizens' offices. This in general has shown the need for a trusted mobile solution. As a more specific result, the existing online ID function could not be activated locally in the Citizens' Office and consequently citizens could not use important administrative services digitally. For this reason, the Federal Government will implement in 2021 a partial digital process for the subsequent activation of the online ID function as well as for subsequent online application for a new PIN.
- Most eID transactions are accounted for by the eServices of pension insurance in the case of official benefits. With their online ID, citizens can access their pension account within seconds –

this can be a great help, for example, in financing talks with banks. Regarding the private sector offers, the unlocking of newly acquired SIM cards or eSIM by mobile operators with the online identification is a frequently used application. It works much faster than video-ident and the SIM card or eSIM can be used immediately. During the Covid 19 pandemic, grid capacity was not sufficient, especially at the beginning of the first lockdown. Video-ident-procedures therefore often failed or were interrupted and had to be restarted. With the online ID, however, the identifications could usually be performed without interference.

4. Ongoing and future Digital Identity reforms

The Federal Government is currently implementing the Digital Identities project. The aims of the project are the development and introduction of electronic identification with the smartphone (Smart-eID) and the creation of a basis for a national and European "self-sovereign identity ecosystem“.

Germany is aiming for an SSI-based identity ecosystem that is EU-compatible and open to both government applications and private sector applications. The national online identity function fulfils the level of assurance high according to the eIDAS regulation and thus forms the ideal basis for any SSI-based identity ecosystem. Additional attributes that are not included in it must be verified by other locations and can thus be used to enrich the digital identity.

As part of the Digital Identities project, the Federal Government is currently working with private sector actors to design an open identity ecosystem based on an SSI wallet. This interdepartmental initiative with the participation of the Federal Chancellery is working on 8 use cases with companies from the mobility, banking, hotel, e-commerce and telecommunications sectors to demonstrate the potential of an SSI-based eID ecosystem before the end of 2021.

A second initiative involves the Federal Ministry for Economic Affairs and Energy and is called "Secure Digital Identities" (2021-2024), in which technical solutions, predominantly SSI, will be tested, harmonized and prepared for rollout in four large-scale showcase projects together with citizens, municipalities and SMEs.

The early involvement of all relevant stakeholders in the public sector and the private sector is of great importance for the success of the introduction of a national offer for electronic identification. The public needs to be informed at an early stage of the new possibilities and offer user-friendly, attractive use cases, especially in the area of economic applications, before the public offer is widely promoted.

Italy

1. National context

Digital identity in Italy relies on a combination of three separate solutions. The Public Digital Identity System (SPID) is the single digital identity used for identity verification in Italy and works in conjunction with the Electronic Identity Card (CIE). In addition, Italians can use the National Services Card (CNS). Although the CNS is not approved and recognised under the EU eIDAS Regulation, it plays an important role in allowing citizens and professionals to have access to digital services.

In Italy, all individuals above 18 years old can request a digital identity. The total population of the country in 2021 was 59.6 million, with the total population eligible for a digital identity (based on age) 50.2 million, or 84% of the total population.

2. Current national Digital Identity management system

The country model

- The Italian Ministry of Innovation and Digital Transition (MITD) is in charge of steering the strategic direction, coordination, evaluation, and implementation of policies and programs in a wide range of policy areas relative to innovation and digitalisation, including digital identity. The Agency for Digital Italy (AgID) is the regulatory body responsible for overseeing the delivery of SPID and identity providers while the Ministry of the Interior is in charge of delivering the CIE.
- For the funding of SPID, Identity Providers (IdP) fund themselves by selling SPID to relaying parties (RP) such as private service providers or other related services, like signature services and professional versions of digital identity. The IdP make a profit only with private service providers. For CIE, users pay approximately EUR 24 to get their identity card and a fraction of this fee is used to sustain services provided by the Ministry of the Interior.
- The identification standards and technical protocols for SPID and CIE both comply with the EU eIDAS Implementing Regulation. The Government assesses and certifies the quality of private identity providers for SPID through an accreditation process carried out by AgID. The legal basis for the assessment carried out by AgID is art. 64 of the Law Decree 285/2014 and art. 64.2of the Code of Digital Administration (CAD). In particular, art. 4 of the Law Decree 285/2014 entrusts AgID with managing the assessment and accreditation process of private IdPs. The accreditation takes the form of a bilateral agreement between AgID and the IdP. AgID (art. 6 of the bilateral agreements) carries out oversight tasks and periodical reviews of each IdP (e.g. compliance with the standards, quality of the service etc.). AgID can also carry out random testing to continuously assess the compliance and quality of the services of the certified IdPs.
- In its current digital identity system, the Italian government collaborates with the private sector mainly in the form of private IdPs. Currently, eight out of the nine IdPs in Italy are private companies. In addition, the government collaborates with banks and financial services providers and software companies. Finally, private companies can use both SPID and CIE as service providers.
- In Italy, the Tax Identification Number is used as a single National Identification Number across all services. It is issued to every Italian citizen at their birth. Every foreign resident or worker also receives a 'Fiscal Code' upon registering with the Italian public authorities.
- Citizens can request access to a digital identity (SPID) through an online-only process. The procedure requires them to provide a valid identity document, the national number (Fiscal Code), a personal mobile number, and an email address. The user can then choose between the IdPs and complete the procedure through their websites. The online-only process is available for most of the IdPs. Depending on the IdP the user applying for SPID is identified via either a) webcam either in a call with a IdP operator or via a video/photo taken to prove his/her identity; or b) online identification with CIE or electronic passport, following the identification procedures through the mobile app of the IdP.
- SPID acts as the single digital identity, which is provided by different IdPs. It allows users to log into different organisations and provides an exchange for identity transactions. SPID is mandatory for authentication for government agencies/departments and optional for the private sector.
- CIE is a smart card that works both as a personal identification document that certifies the identity of the holder, and as a means of authentication for online public and private service providers. 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. By law, CIE is progressively replacing the paper Identity card.
- CNS is a smart card or a USB key containing a 'digital certificate'. CNS is issued by the Italian Revenue Agency or alternatively by a Chamber of Commerce. CNS allows users to prove their

identity online and to access digital public services (e.g. digital health services and financial services). In addition, the CNS issued by the Chamber of Commerce allows businesses to sign digital documents (financial statements, bills, contracts etc.) and to access digital public services for businesses.

Technical choices

The different means for authentication used in Italy include smartcards; digital certificate files; e-signatures; username and password; and two factor authentication (2FA) that confirms access to email account, mobile phone number, or mobile device.

Authentication via SPID is designed around three security levels:

1. **Username and password:** the first level allows the user to access online services through a username and a password chosen by the user.
2. **2FA:** together with the password, the user will be requested to access through a temporary one-time password (OTP) that will be sent to the user's phone number (SMS) or mobile device (application provided by IdP).
3. **3FA:** username and password plus physical device that handles cryptographic keys (e.g. smart card)

Italy considers username and password useful for increasing the user-friendliness of digital public services, especially for people with basic digital skills. The single-step authentication constitutes an immediate and intuitive means to access remotely digital public services. Furthermore, it might be particularly adequate and useful for 'low-risk' and 'low-impact' scenarios where improper use of digital identity services would result in a negligible damage to the citizen or the business.

1.5% of the population that has a digital identity uses a smartcard to authenticate themselves and per month, 2 million authentications are issued using a smart card. According to Italy, smartcards are especially useful for those who own an NFC mobile phone.

2FA is considered particularly valuable for accessing the services of public administrations. Most public services require 2FA in order for the user to access them. The heightened level of control responds to the need of providing certainty on the identity of the user and minimizing risks when sensitive personal information is being accessed. 2FA confirming access to a mobile phone number responds to Italy's strategy of moving towards an increasingly mobile digital government that values the portability and availability on mobile devices of digital identities. As the majority of access to digital identity (SPID) takes place through smartphones, linking the 2FA to a mobile phone number increases the usability and user-centricity of the service as it allows the user to complete the operation through a single device.

Portable (cross-platform, cross-sectoral, cross-border) digital identity

- **Cross-platform:** As described above, SPID and CIE are available through smartphones and other mobile devices. Italy is expected to establish closer collaboration with Mobile Network Operators when developing a mobile digital identity.
- **Cross-sectoral:** In Italy, a non-public sector organisation (including the private sector) can develop and provide a service that relies entirely on available digital identity solutions to function. Of all the possible non-public sector services (private sector and other providers of services) that could be using available digital identity solutions, between 1-24% are doing so. The remaining services are using identification through personal credentials via a website or mobile app (e.g. personal number and/or two-step-identification are required to access most of the online banking services), or in-person identification through paper documents. AgID supports the SPID implementation process.

- **Cross-border:** The Italian eIDAS-Node enables the cross-border interoperability of digital identity (eID) systems and the circularity of eIDs in EU member states. In 2021, in practice, digital identities from 23 EU/EEA member states could be used to log in to public and private digital services in Italy: Portugal, Finland, Croatia, Austria, Denmark, United Kingdom, Luxembourg, Latvia, Slovenia, Netherlands, Slovakia, Czechia, Ireland, Lithuania, Malta, Spain, Estonia, Sweden, Greece, Cyprus, Germany, Belgium, and Norway. Within the EU acquis, the Proposal for a Regulation amending Regulation (EU) No 910/2014 as regards establishing a framework for a European Digital Identity (COM(2021) 281 final) put forward by the European Commission on 3 June 2021, is expected to provide further guidance to the development of digital identities at both the Member State and Union-wide level.

Data visibility and citizen consents

In Italy, citizens have a legal right to opt out of the use of a digital identity.

The European Regulation (EU) 2016/679 ('GDPR') provides the legislative framework applicable to personal data connected to the use of the digital identity system. The Italian Data Protection Authority (DPA) oversees the digital identity system compliance with national and European legislation. DPA is an independent administrative authority established by the so-called privacy law (Law No. 675 of 31 December 1996) and regulated subsequently by the Personal Data Protection Code (Legislative Decree No. 196 of 30 June 2003) as amended by Legislative Decree No. 101 of 10 August 2018, which also established the Italian DPA as the supervisory authority responsible for monitoring application of the General Data Protection Regulation (pursuant to Article 51 of Regulation No. 2016/679). DPA is funded with approximately EUR 32 million annually and is staffed with over 320 employees from different backgrounds.

On the SPID website, users are provided with information about the processing of their personal identifiable data from using the digital identity. The user can read about how SPID will use its personal data, how long personal data will be retained, and on the meaning of the relevant legal terms (e.g. consent is defined as the expression of a user's will and it has to be free, specific, informed and unambiguous through which the user expresses its consent to the use, re-use, and sharing of data).The users are informed that all expressions of consent can be revoked at any time. The revoke of one's consent does not affect the lawfulness of data use before the consent was revoked.

Personal data through SPID are handled by AgID. In delivering the relevant services, AgID handles data together with a number of responsible data handlers. AgID does not transfer personal data to third parties, third countries, or international organisations. To ensure the security of user data in private sector digital identity solutions, AgID oversees and has sanctioning power. The Operator ('Gestore') is legally bound through a contract concluded with AgID to continuously monitor, following criteria of necessity and proportionality, how data is being used "in order to detect and tackle potential violation, duplication, and any other abuse of each user's digital identity credentials"

3. Uptake and adoption of Digital Identity

In Italy, it is mandatory for public sector organisations to use SPID for service user authentication and verification, while it is optional for the private sector. Art. 64 of the Digital Administration Code provides that all government services should replace any previous authentication models with SPID, with the exception of CIE. The SPID implementation process is assisted and supported by AgID. Out of all public sector services where it would be necessary to authenticate users, 50-74% were using it in 2021. On average, individuals use a digital identity to access or consume public services 24 times per year.

In December 2019, prior to the COVID-19 pandemic outbreak, the number of individuals with a digital identity was 5.5 million. The percentage of the eligible population that had a digital identity was therefore

11%. In April 2021, a year after the first wave of the pandemic, the total population with an active access to a digital identity was 20.3 million[40], meaning digital identity adoption had increased by 269% to 40%.

- Efforts have been made to simplify the activation of SPID for citizens by working through administrations which have, since October 2020, had a regulatory obligation to activate SPID and CIE for citizens. According to the Public Registration Authority Officer (RAO) model, citizens can visit an administration for their identity to be checked, free of charge, in order to pass the first phase of identification for a SPID. Administrations have received economic incentives from an Innovation Fund to support this process. In April 2021 there were 24 active administrations.
- A further important contribution made by SPID during 2020-21 was as an 'enabling platform' to the IO app. The IO App debuted in April 2020 and is the app for Italian public services, which represents a single channel through which all local and national authorities offer their services to citizens directly on smartphones. As of April 2021, IO had been downloaded over 11 million times. SPID constitutes the most used and least burdensome way to access the IO app. The IO app allows citizens to benefit from further benefits such as:
  - Cashback - a 10% cashback on purchases with payment cards and apps registered on IO, as part of the “Cashless Italia” plan promoted by the Italian Government to reduce use of paper money and foster a more widespread adoption of digital payments. From December 8, 2020, more than 465 million transactions were processed by almost 8.5 million people, who added a total of 15.3 million payment methods.
  - *Bonus Vacanze* - a subsidy of up to 500 euros for citizens to support domestic tourism during the pandemic. From July 1, 2020, through IO 1,885,802 families obtained the *Bonus Vacanze* in less than 3 minutes on average (2.2 minutes in 80% of cases) and benefits were disbursed for an economic value of 829,431,050 euros.
- Italy recognises that the introduction of a new identification scheme needs time to be adopted and needs to be communicated properly to the population. The rapid uptake of SPID has mostly been linked to the provision of new services on digital platforms accessible through SPID. Top-down governmental communication on new services being introduced has been instrumental in accelerating the digital identity uptake. The provision of new services and communication thereof in the press, TV, and social media, in particular welfare measures linked to the COVID-19 Recovery packages passed by the Government in 2020, proved instrumental in encouraging the uptake of digital identity. The launch of initiatives such as the '*buono vacanze*' ('Holiday bonus') and the 'cashback scheme' acted as an accelerator for the adoption of SPID digital identity.
- During the COVID-19 crisis, SPID allowed access to online public services and financial support made available by the government. Alongside the availability of new services using SPID prompted by the pandemic, the *Decreto Semplificazioni* reflected the strong push by the government to mandate the use of SPID and CIE by public service teams. In 2020, some public sector organisations anticipated the deadlines of the Decree: for example, the Ministry of Labor and the National Institute of Social Security (INPS), which is the largest social security and welfare institute in Italy with approximately 200 online services for citizens with authentication, started the transition from PIN to SPID and CIE in October 2020. The INAIL(National Institute for Insurance against Accidents at Work) and the *Agenzia delle Entrate* (Italian Revenue Agency - which has about 200 online services with authentication) have also started the transition from their own in-house credentials to the use of SPID and CIE, in line with the timing of the Decree.

[40] As of June 2021, 21 207 235 CIE cards have been activated and 21 540 028 SPID had been issued. However, given that individuals can have both a CIE and a SPID, the total number of Italian citizens and residents owning a digital identity is lower than the sum of the two. The reported figure in the text reflects the number of CIE *or* SPID issued. This means that the figure likely underestimates the total number of individuals in Italy with a digital identity (either CIE or SPID) in April 2021.

4. Ongoing and future Digital Identity reforms

The Italian government is currently working to improve SPID. In particular, the federal government is working to find ways of collaborating and coordinating with central and local entities more effectively, especially with regard to the delivery of specific and useful online services that would improve the number of citizens who adopt SPID or CIE. The Strategy 'Italia 2026' announced in April 2021 by the Minister of Innovation and Digital Transition aims at strengthening the uptake of digital identity (both CIE and SPID) in Italy. The Strategy aims at the adoption of digital identity by 70% of the adult population by 2026.

The Strategy is consistent with the EU-wide targets put forward by the European Commission's Communication "2030 Digital Compass: the European way for the Digital Decade". In addition, Italy will leverage on the EU Recovery and Resilience Facility's funds to strengthen its digital identity system. In particular, CIE and SPID are expected to gradually become enabling platforms for a broader digital identity architecture.

Italy furthermore aims at integrating its national digital identity with a self-sovereign digital identity wallet issued through mobile solutions, compliant with upcoming European legislation (Proposal for a Regulation amending Regulation (EU) No 910/2014 as regards to establishing a framework for a European Digital Identity (COM(2021) 281 final), 3 June 2021.

Indonesia

The Indonesian approach to digital identity has been in place since 2013 with the digital identity solution in electronic databases using Indonesia’s Single Identity Number as the primary key.

At the moment, the digital identity solution for authentication and verification is implemented through digital certificate file and e-signatures.

More than 3000 stakeholders from the public and private sectors have been involved in a cooperation agreement with the Directorate General of People Registry and Civil Registration of the Indonesian Ministry of Home Affairs to integrate, verify, and validate data in the implementation of digital identity. Up until July 2021, the verification processes in the General Directorate of People Registry and Civil Registration has been completed 7 billion times, or 1-5 million times a day as a result from the cooperation agreement between the Ministry and corresponding stakeholders.

The government intends to continuously improve the system through data utilisation, data interoperability, big data centralisation, as well as the implementation of smart card.

Indonesia’s digital identity is underpinned by Government Regulation No.40 of 2019 on the Implementation of Act No.24 of 2014 of People's Civil Registration and Administration, and Government Regulation No. 71 of 2019 on Electronic System and its implementing regulation. For the latter regulation, it governs the prerequisite for an e-Certificate provider, which may include provision of Digital Signature, which may potentially be utilised as Digital Identity.

The development of digital identity is considered a priority area and will be carried out in conjunction with the establishment of personal data protection legislation which is also under development. These two areas are reflective alongside one another. In developing digital identity, Indonesia will further seek the benefits derived from international standards.

Mexico

Mexico is currently working on implementing its digital identity scheme including new laws to facilitate the transition. Today there are different isolated digital identity schemes in place. The *Clave Única de Registro*

de Población (CURP) or the Unique Population Registration Code in English, is the national identification number used to access public sector and private sector services and it is assigned to all Mexican citizens.

During the COVID-19 pandemic, the CURP has been of great value in terms of the administration of vaccination to the population. The most important lesson from the pandemic in relation to the development of digital identity is that the civil registry needs access to quality information and must have close collaboration with health sector institutions.

Russia

1. National context

The current national digital identity of Russia is called the Unified Identification and Authentication System and is available to individuals aged 14 or above can have a digital identity. The system makes provision for the use of biometric data.

Russia's total population in 2021 was 146.2 million, and the total eligible population for digital identity based on age was therefore 122.3 million, or 84% of the total population.

2. Current national Digital Identity management system

The country model

The digital identity model in Russia is for sector specific digital identity solutions with a reusable public sector digital identity. This means there are private sector solutions for accessing private sector services and a public sector solution that can be used for accessing both public and private sector services.

- The Russian Ministry of Digital Development, Communications and Mass Media of the Russian Federation is in charge of steering the strategic direction and overseeing delivery of digital identity in the country
- The identification standards and technical protocols for digital identity in Russia are set out by the Unified Identification and Authentication System. Methodological recommendations for the use of the Unified Identification System and Authentication Version 2.84 (2021) and Methodological recommendations for integration with the REST API of the Digital Profile. Version 1.16. (2021)
- The Russian digital identity can be obtained through an online-only process.
- Russia does not have a single unified identification number that is used across all services.

Technical choices

The different means for authentication used in Russia include e-signatures and username and password

Portable (cross-platform, cross-sectoral, cross-border) digital identity

- **Cross-platform:** Russia's digital identity can be used on mobile devices.
- **Cross-sectoral:** No information was provided about private sector usage of the national digital identity solution
- **Cross-border:** Although Russia has no provision for recognising foreign digital identity solutions or enabling its reuse elsewhere, the Federal Law "On Personal Data" dated July 27, 2006 No. 152-FZ, provides for a regulation concerning the conditions for the cross-border transfer of personal data. According to Article 12 of the Federal Law, data transfer (cross-border data flow) can be

carried out to the territory of foreign states that provide adequate protection of the rights of subjects of personal data. These states include:

- member states of the Council of Europe Convention No. 108 "On the Protection of Individuals with regard to Automatic Processing of Personal Data" (hereinafter - Council of Europe Convention No. 108);
- states not party to the Council of Europe Convention No. 108 and ensuring adequate protection of the rights of subjects of personal data, included in a special list under the order of *Roskomnadzor* dated March 15, 2013 No. 274 "On approval of the list of foreign states that are not parties to the Council of Europe Convention for the Protection of Individuals with regard to Automated Processing of Personal Data and ensuring adequate protection of the rights of subjects of personal data ".

Data visibility and citizen consents

In Russia, citizens have a legal right to opt out of the use of a digital identity. In accordance with clauses 18.16 and 18.21 of Article 3 of the Federal Law of December 29, 2020 No. 479-FZ "On Amendments to Certain Legislative Acts of the Russian Federation", the refusal of an individual to undergo identification and (or) authentication using his biometric personal data cannot serve grounds for refusing to provide him with state or municipal services and services.

The following legislation exists to protect a person's data connected to the use of a Digital Identity system:

- Federal Law 63-FZ "On Electronic Signatures";
- Federal Law 115-FZ "On Counteracting Legalization (Laundering) of Criminally Obtained Incomes and Financing of Terrorism";
- Federal Law 126-FZ "On Communication";
- Federal Law 149-FZ "On information, information technology and information protection";
- Federal Law 210-FZ "On the organization of the provision of state and municipal services"
- Federal Law 152-ФЗ "On Personal Data" dated July 27, 2006 (as amended on 12/30/2020);
- Federal Law 259-FZ "On crowdfunding in Russia using investment platforms" dated August 2, 2019;
- Federal Law 482-FZ "On Amendments to Certain Legislative Acts of the Russian Federation" dated December 31, 2018, which establishes the legal basis for the collection of biometric personal data of Russian citizens and their placement in the Unified Biometric System.

In Russia there is an independent authority monitoring and overseeing the impact of Digital Identity on individual privacy and freedoms. The Ombudsmen for Human Rights in the constituent entity of the Russian Federation. In case of complaints from citizens of the Russian Federation, foreign citizens or stateless persons about violation of the rights to private life and human freedom, the human rights ombudsman applies the procedure established by the Federal Law of May 2, 2006 No. 59-FZ "On the Procedure for Considering Appeals from Citizens of the Russian Federation ", taking into account the specifics of accepting for consideration and consideration of complaints by the human rights ombudsman in the constituent entity of the Russian Federation, established by Federal Law No. 48-FZ of March 18, 2020" On Ombudsmen for human rights in the constituent entities of the Russian Federation ").

Protections exist to ensure that private sector actors cannot commercialise data obtained from Digital Identities without a user's consent. In accordance with Article 7 of the Federal Law "On personal data" dated July 27, 2006 No. 152-FZ, operators and other persons who have gained access to personal data are obliged not to disclose to third parties and not to distribute personal data without the consent of the subject of personal data, unless otherwise provided by federal law. In addition, in accordance with Article 5 of Chapter 2 of the Federal Law "On Personal Data" dated July 27, 2006 No. 152-FZ, the processing of

personal data should be limited to the achievement of specific, predetermined, and legitimate goals. Processing of personal data that is incompatible with the purposes of collecting personal data is not allowed. Administrative liability is provided for violations of the law.

The security of user data in private sector Digital Identity solutions is covered under the requirements of the Federal Law "On Personal Data" dated July 27, 2006 No. 152-FZ. Both public and private providers bear the same responsibility as provided for by the legislation of the Russian Federation.

Russian citizens are not proactively informed by authorities about any processing of their personally identifiable data. However, users can access and see what attributes or data are being shared/re-used, and with/by whom. In accordance with paragraph 7 of Article 14 of the Federal Law "On personal data" dated July 27, 2006 No. 152-FZ, the subject of personal data has the right to receive information regarding the processing of his personal data, including information containing:

- confirmation of the fact of processing personal data by the operator,
- legal grounds and purposes of processing personal data,
- goals and the methods of processing personal data used by the operator,
- the name and location of the operator,
- information about persons (except for the operator's employees) who have access to personal data or to whom personal data may be disclosed on the basis of an agreement with the operator or on the basis of federal law,
- the processed personal data related to the relevant subject of personal data,
- the source of their receipt.

Unless another procedure for submitting such data is provided for by federal law, processing of personal data, including the terms of their storage, the procedure for exercising by the subject of personal data the rights (provided for by this Federal Law), information about the carried out or about the intended cross-border data transfer, the name or surname, name, patronymic and address of the person who processes personal data on behalf of the operator, if the processing is entrusted or will be entrusted to such a person, other information provided for by this Federal Law or other federal laws.

Russian citizens can provide and revoke consent for the re-use and sharing of attributes or data originating from their Digital Identity.

Civil society organisations are not able to monitor the process by which a person's identifiable data is shared and reused.

The processing of a person’s identifiable data is governed in terms of proportionality or legitimacy according to Article 5 of the Federal Law of July 27, 2006 No. 152-ФЗ "On personal data". This covers the following principles:

- processing of personal data should be carried out on a legal and fair basis;
- the processing of personal data should be limited to the achievement of specific, predetermined, and legitimate purposes. (Processing of personal data that is incompatible with the purposes of collecting personal data is not allowed);
- only personal data that meet the purposes of their processing are subject to processing;
- the content and volume of the processed personal data must correspond to the stated purposes of the processing. (The processed personal data should not be redundant in relation to the stated purposes of their processing);
- when processing personal data, the accuracy of personal data, their sufficiency, and, if necessary, relevance in relation to the purposes of processing personal data must be ensured. (The operator must take the necessary measures or ensure their acceptance to remove or clarify incomplete or inaccurate data).

3. Uptake and adoption of Digital Identity

In December 2019, prior to the COVID-19 pandemic outbreak, the number of individuals with a digital identity was 103 million. The percentage of the eligible population that had a digital identity was therefore 84%. No data was supplied relating to adoption figures following the pandemic.

However, in Russia it is not mandatory for public sector organisations to use the national digital identity solution. Annually, 230 million authentication events are registered using the system.

4. Ongoing and future Digital Identity reforms

There is a huge increase in demand for remote identification due to COVID-19.

Various cases using biometrics for individuals and legal entities are being piloted within the framework of the FinTech Association projects "Remote Identification" and "Digital Profile", together with banks and insurance companies. For example, remote identification of clients and opening an account. In addition, proposals for legal regulation and standardization are being worked out.

The ongoing, and increasing, costs associated with verifying the digital identity of a person (a set of technologies and smart devices that make it possible to verify a person using digital information: biometrics, digital passports, IDs, passwords, PIN codes, QR codes) will continue. This factor must be taken into account when forming the corresponding budgets. It can be assumed that COVID-19 will launch a wave of legislative changes around the world and as a result, the possibilities for using remote identification will expand. At the same time, the technologies themselves will change. On the one hand, the fight against the coronavirus will lead to a sharp decline in the use of fingerprint scanners for personal identification, since these devices must be touched with a hand. There will also be requirements for the use of antimicrobial materials in such terminals.

Saudi Arabia

1. National context

In Saudi Arabia, citizens above 10 years old can request a digital identity. The total population of the country in 2021 was 35 million, with the total population eligible for a digital identity (based on age) 24.4 million, or 70% of the total population.

2. Current national Digital Identity management system

The country model

The IAM system in Saudi Arabia is centralised with third party IdPs brokers. Authentication is made based on assurance levels, either using two factors (National ID / Password, SMS) for major public services, or using biometrics/digital certificates based on service criticality (risk-based assessment). Currently there are no differences in services provided for either public or non-public sector except that non-public sector usage gets charged compared to public services which are offered for free.

The Digital Government Authority (DGA) steers the strategic direction for and vision of digital identity in the country, and the Saudi Data and Artificial Intelligence Authority (SDAIA) oversees the delivery of the digital identity, including IdPs. The government provides funds for government IdP to provide services to the public sector free of charge, whereas private IdPs brokers are self-funded since they are generating revenues through transaction cost.

There are a set of standards in place in Saudi Arabia related to digital identity life-cycle management, digital certificates, technical standards for identity and access management (IAM) technologies, and biometric technologies. The Saudi government assesses and certifies the quality of private identity providers in line with the identification standards through periodic audits as set in agreements with IdP's. The Saudi government collaborates with the private sector in order to contribute to the digital identity on boarding process and by acting as third party IdPs brokers, including IdPs and banks and financial services providers.

Users in Saudi Arabia can obtain a digital identity through an online-only process. For individuals, they must first link their mobile number to a digital identity account using either KIOSKs (which are distributed across the country) or through the digital identity website to provide their information. In Saudi Arabia, the civil registration systems act as the national identification number to connect records across services. As for businesses, the owner needs to have a digital identity before requesting to issue a commercial registration. Then he would follow the same steps as an individual using the business option on the website.

Technical choices

The means for authentication of a digital identity in Saudi Arabia include smartcards, digital certificate file, and two-factor authentication that confirms access to a mobile phone number or that requires access to biometric information.

- Per month, approximately 5000 authentications/verifications are issued with a smartcard by any available digital identity solution
- 1.1 million authentications/verifications are issued per month with two-factor authentication that requires access to a mobile phone number.
- There are no available figures on the number of authentication/verifications issued that require access to biometric information. The most common service requiring biometric information is notarization services. Biometric data are stored as per related standards, and only qualified readers are allowed to be used.

Portable (cross-platform, cross-sectoral, cross-border) digital identity

- **Cross-platform:** The digital identity solutions in Saudi Arabia can be accessed from different mobile devices.
- **Cross-service:** In Saudi Arabia, non-public sector organisations can use the available digital identity solution for service user authentication/verification.
- **Cross-border:** A technical team represents the member countries in the Gulf Cooperation Council (GCC) responsible for integrating national digital identity systems in GCC countries. This technical team is supervised by a ministerial level committee from GCC countries within the council. As of today, the digital identity system of Bahrain is fully integrated with the Saudi digital identity system. Saudi Arabia is in the process of integrating its system also with the United Arab Emirates, Qatar, Kuwait and Oman. For Saudi Arabia, when agreeing to mutual recognition of Digital Identity between countries, they use legislation and policy mapping to establish the extent to which privacy protection and data security approaches of the other country are consistent with their domestic policies. GCC countries share some mandatory laws or model laws that facilitate this process.

Data visibility and citizen consents

In Saudi Arabia, individuals do not have a legal right to opt out of the use of digital identity.

Saudi Arabia has established the National Data Management Office (NDMO) as the national regulator of data in the Kingdom, NDMO has developed the framework for national data governance to set the policies and regulations required for data classification, data sharing, data privacy, Freedom of Information, open data and others.

Today, citizens are not proactively informed by authorities about the processing of their data. Users are not able access and see what attributes or data are being shared/re-used, and with/by whom, nor provide and revoke consent for the re-use and sharing of attributes or data originating from their digital identity.

3. Uptake and adoption of Digital Identity

In Saudi Arabia, it is mandatory for public sector organisations to use the available digital identity solutions for service user authentication and verification. To support public sector teams in adopting digital identity solutions, they are provided with awareness sessions, integration guides, software integration tools, technical support, legal documents, and service-level agreements. As of today, 75%-99% of public sector services where it would be necessary to authenticate users are using available digital identity solutions. The other services are still using other previously built means of authentications (mostly username/password, SMS). On average, individuals use the available digital identity solution to access or consume any public sector service 49 times per year.

In December 2019, prior to the COVID-19 pandemic outbreak, the number of individuals with a digital identity was 16 million. The percentage of the eligible population that had a digital identity was therefore 66%. In April 2021, a year after the first wave of the pandemic, the total population with an active access to a digital identity was 21 million, meaning the share of eligible population with a digital identity had increased with roughly 20 percentage points to 86%.

During the COVID-19 pandemic, Saudi Arabia benefitted from digital identity to help organize the curfew and issue permits to individuals to help control quarantine and the spread of COVID-19. Almost all sectors including digital payment, health services, commercial, retail, ICT, Judicial and more benefitted from digital identity to meet needs during the pandemic. The most important lesson learned for Saudi Arabia from the COVID-19 pandemic in relation to the development and use of digital identity is the value of trusted, portable and cross-platform digital identity solutions.

4. Ongoing and future Digital Identity reforms in Saudi Arabia

Saudi Arabia is developing a national strategy for digital identity, comprising Governance Model, Digital identity and trust services, Operating model and service delivery, Legislation, Standards, Return on investment and liquidation, and technical architecture. Furthermore, the country is updating the e-transaction law (draft Digital Transactions and Trust Services Law) to add more legal provisions related to digital identities and trust services, and to harmonize with other international laws like e-IDAS and UN model laws.

Saudi Arabia has plans to pursue self-sovereign identity in the future, which are detailed in the current national strategy for digital identity.

The biggest lessons learned by Saudi Arabia from their digital identity reforms include

- That harmonization of digital identity regulations is key to achieve interoperability and cross-borders online services.
- That it is paramount to align government and private entities on strategy and direction for digital identity
- The need for clear governance that covers digital identity regulations, digital identity service providers, data privacy regulation, sustainability models, investment models, etc.

Singapore

1. National context

Singpass and Corppass are the national digital identities of Singapore for natural persons and corporate entities. The total population of Singapore is 5.6 million. Individuals can obtain the SingPass at 15 years of age, meaning that the total eligible population for SingPass is 4.2 million people or 75% of the total population.

2. Current national Digital Identity management system

The country model

Singapore's National Digital Identity (NDI) is a Strategic National Project implemented and managed by the Government Technology Agency (GovTech) under the Smart Nation Digital Government Group (SNDGG). SNDGG was formed in 2017 housed under the Prime Minister's Office.

The development of the Singapore's National Digital Identity is funded by the government.

Singapore's NDI assurance level references a combination of NIST IAL and AAL, as well as multiple authentication factors to provide higher assurance when required. Higher NDI assurance level could be achieved by using a combination of more than one authentication factors offered by Singpass (e.g. Singpass app with Face Verification with Singpass). Singpass supports "stepped-up" authentication (use of additional authentication factors for high risk/value transactions).

Private sector organizations play the role of a Relying Party that integrates and adopts Singpass products. Private sector organizations could also integrate the Sign with Singpass into their product to offer digital signing as a commercial solution.

NDI serves as a digital infrastructure and trust platform that enables Singapore residents and businesses to transact digitally with the Government and private sector in a convenient and secure manner. As a result of this government led initiative, private sector companies can tap on the NDI digital infrastructure to obtain high identity assurance online, verified against authoritative government data sources without building infrastructure from scratch. To allow government agencies and businesses to access NDI's Trusted Services, we have introduced Singpass app, a mobile application that users mainly interface with, and seven application programming interface (api) products namely Authorise, Identiface, Login, Myinfo, Notify, Sign, and Verify on the NDI platform.

Singapore residents and businesses can tap on the Myinfo API product to share government originated personal and corporate information upon consent. Some use cases are identifying yourself when applying for a bank loan online and proving of identity in a physical setting with digital identity cards. Singpass Face Verification API product – Identiface, enables businesses to adopt face verification technology without the need to set up. The single National Identification Number used across all services are retrieved from the Singapore government, Immigration & Checkpoints Authority

Users can obtain the Singpass through an online-only process:

- Users will first check for eligibility and register for Singpass at www.singpass.gov.sg
- The user's Singpass password will be mailed to the user's local registered address
- To complete the setup process, the user will need to log into their account using the mailed password via the Singpass portal or Singpass app
- Upon successful login, the user's account will be activated and complete the online application process.

The Singaporean government is in the process of implementing Face Verification to augment the onboarding of users.

Technical choices

The means used for authentication in the national digital identity system include digital certificate, E-signatures, username and password, and two-factor authentication that confirms access to an email account, a mobile phone number, a mobile device, or that requires access to biometric information.

- 100% of the population that has a digital identity uses digital certificates and per month 8.5 million authentications are issued with this means.
- 64% of the population that has a digital identity uses E-signatures and per month 37 000 authentications are issued with this means.
- 5% of the population that has a digital identity uses username and password, and per month, 900 000 authentications are issued with this means.
- 25% of the population that has a digital identity uses two-factor authentication that confirms access to a mobile phone number, and per month, 2 million authentications are issued with this means.
- 70% of the population that has a digital identity uses two-factor authentication that confirms access to a mobile device, and per month, 8.5 million authentications are issued with this means.
- 70% of the population that has a digital identity uses two-factor authentication that requires access to biometric information, and per month, 17 000 authentications are issued with this means.

Portable (cross-platform, cross-sectoral, cross-border) digital identity

- **Cross-platform:** The national digital identity of Singapore can be used through different mobile devices and is therefore considered cross-platform portable.
- **Cross-sectoral:** Singpass can be used by both public and private sector service providers to authenticate the identity of service users and is therefore considered cross-sectoral-portable.
- **Cross-border:** Singapore does currently not recognise any other country's digital identities for service user authentication and verification.

Data visibility and citizen consents

Singapore’s Personal Data Protection Act (PDPA) regulates the process of personal data in Singapore.

Citizens are proactively informed about the processing of their personal data by government authorities. Users can access the transaction history of Myinfo in the Singpass app to see what attributes or data are shared, and who the data is shared with. For Myinfo data transactions, the digital service will direct the users to authenticate themselves using Singpass. Upon successful authentication, the user will be redirected to a consent page where the transaction purpose, and data items requested will be shown to the user. Upon consent, the user completes the transaction and a notification will be sent to the user showing a list of data items involved in the transaction. This information on the attributes or data that are shared and who the data is shared with are also made available in the Singpass app.

Users are required to give consent before using biometrics for authentication purposes. When the system captures a user’s facial image, it is compared against the Government’s biometric database (e.g. NRIC, Singapore Passport or Work Pass photo) for authentication purposes. Liveness detection technology solutions are incorporated into the authentication process to detect fraudulent access involving the use of photographs, videos, or masks. All captured facial images are encrypted and protected with advanced technologies to prevent unauthorised access. Additional measures, such as security incident monitoring, are also put in place to ensure that a user’s personal data is securely protected. Relying parties would

receive a verification result after comparison. They do not need to build, secure and maintain biometric databases. The Government systems will only keep the captured facial images for 30 days for audit purposes. Thereafter, the images will be deleted. The user's data will not be used for any surveillance or commercial purposes.

For every data sharing transaction with the private sector, all users must give their consent in order to complete the transaction. Prior to onboarding of the private sector service, these use cases are screened by the government. Private sector actors are also required to comply with Singapore's PDPA (Personal Data Protection Act), which permits the disclosure of information only with consent of the individual.

Because of contact tracing efforts, public officers and contact tracers require access to sensitive personal information. Singapore reports that the rapid roll out of new technology presents risks in Data Governance and Data Security:

- Knowingly or reckless data disclosure without authorisation;
- Data misuse that results in personal gain for the public officer or another person, or harm or loss to another person
- Knowingly or recklessly re-identify anonymised information without authorisation.

The COVID (Temporary Measures) Act ("CTMA") specifies that public sector agencies can use personal contact tracing data recorded in digital contact tracing systems (such as TraceTogether (TT) and SafeEntry (SE)) only for the purpose of carrying out contact tracing, except where there is a need for police officers and law enforcement officers to use the data for criminal investigations and proceedings in respect of seven categories of serious offences. These are offences of a significant severity and/or pose an immediate threat to life or public safety, such as use of firearms and dangerous weapons, terrorism, murder, drug offences that attract death penalty, kidnapping and rape. These categories of offences are set out in the Seventh Schedule of the CTMA and the Government cannot amend the list of offences without Parliamentary approval. The CTMA covers personal contact tracing data – proximity data, locations visited, and user information collected through SE or TT, and which is able to identify an individual. The legislation specifies the following safeguards:

- No further collection will be allowed as soon as the pandemic ends and all data collected thus far will be deleted as soon as practicable,
- The Government may not use the data for any purpose other than those specified in the CTMA, regardless of any other written law requiring or allowing the disclosure of the data.
- Stiff penalties are meted out for any contravention of the Act (up to 2 years' imprisonment or up to $20,000 fine)

The legislation is the result of a delicate balance between the right to public health, the right to public security and respecting the sensitivity of personal data during this extraordinary time of an ongoing pandemic.

Administratively, the Government has robust internal policies and guidelines on data governance, and especially so for personal and contact tracing data. In 2019, the Government also convened a Public Sector Data Security Review Committee (PSDSRC) to review how the Government is securing and protecting citizens' data from end-to-end, and to recommend measures and an action plan to improve the Government's protection of citizens' data and response to incidents. Public agencies with access to the personal digital contact tracing data are obliged, by way of the Public Sector (Governance) Act, to safeguard the data in accordance with internally-prescribed data security requirements. These include the recommendations made by the Public Sector Data Security Review Committee in 2019.

3. Uptake and adoption of Digital Identity

- In Singapore, it is mandatory for public sector organisations to use the National Digital Identity for service user authentication and verification. Today, 75%-99% of all public services where it is necessary to authenticate users are using the national digital identity solution, remaining services are using manual registration based on details on Physical Identity Card. On average, individuals use the Singpass 50 times per year to access any public service. In order to support public sector teams, An Inter-Ministerial Committee oversees Singapore's National Digital Identity programme. The strong political support facilitates the adoption and implementation of NDI across the public sector. Public sector teams can also access the Singpass API portal (https://api.singpass.gov.sg) to access resources to onboard onto the various Singpass products (National Digital Identity solution). These resources include an API library, onboarding tutorials and guidelines, technical specifications, implementation templates and sandbox APIs to encourage ease of onboarding. The combination of strong political support and support for technical implementation is instrumental to the successful implementation of National Digital Identity across the public sector.
- Non-public sector teams can access the Singpass API portal (https://api.singpass.gov.sg) to access resources to onboard onto the various Singpass products. These resources include an API library, onboarding tutorials and guidelines, technical specifications, implementation templates and sandbox APIs to encourage ease of onboarding.
- In April 2019, during the beginning of the COVID-19 pandemic, 872 000 individuals or 21% of the eligible population had a Singpass. In April 2021, the share of eligible population with the Singpass had increased with 210% to 2.7 million people, which is 64% of the eligible population
- The National Digital Identity programme supported the digitisation of contact tracing processes. SafeEntry is an example of a product that builds on the foundation of NDI. Its objective is to enable authorised contact tracers to quickly obtain identity information of visitors to a physical location. This information is used as a credible reference to uncover locations visited by confirmed cases, identify possible clusters and identify locations for deep cleaning. To use SafeEntry, users give their consent to the transfer of personal information upon scanning a SafeEntry QR code to check in whenever they visit a location.
- Digital readiness has enabled Singapore to respond quickly to the pandemic. With a ready digital infrastructure, Singaporean residents could have seamless and secure digital access to government services without physical interactions. This helped to significantly mitigate some of the disruptions arising from the necessary public health measures in response to tackling the pandemic.

4. Ongoing and future Digital Identity reforms

NDI aims to be secure and widely adopted by citizens and businesses to exchange information and enable hosting other transactions that require identification. From an identity management tool that allowed secure access to government services only, NDI has evolved to enable everyday transactions for citizens (e.g. signing off the receipt of a delivery package) and high value transactions that require highly verifiable, non-repudiable digital signatures (e.g. purchase of insurance).

In addition to a National Digital Identity for individuals and Corporate Digital Identity for businesses, Singapore is progressively building a mobile version of a Corporate Digital Identity for businesses. This with the aim to cater for the increasing volume of electronic corporate transactions by introducing a corporate alternative to an individual's digital identity and enabling corporations to leverage our Digital Signature products.

Singapore is looking to establish cross border interoperability with other countries, i.e. for our National Digital Identities to be compatible with other countries', and vice versa. Identity verification is often needed

in cross-border transactions, such as visa applications, business registration, etc. These processes are onerous and time-consuming, and it is a pain point that having interoperable Digital Identities can address.

Singapore is exploring the extension of its current Digital Identity system to include decentralized identity especially for cross border transactions. Singapore considers that governments can continue to play the role of being a trust digital identity provider in a decentralised digital identity system.

Spain

1. National context

Documento Nacional de Identidad electrónico (DNIe) is the Spanish national electronic ID card used for digital identification of natural persons. The electronic DNI is a proof of identity which is acknowledged by the Kingdom of Spain as the official electronic accreditation document corresponding to the personal identity of its holder and to the electronic signing of documents[41].

Spain's population is 47 million, with 42 million people or 89% of the total population eligible for the DNIe.

2. Current national Digital Identity management system

The country model

The country model for digital identity in Spain is a shared model where the management of digital identity is handled through a partnership between public and private sectors and where the identity itself is used to access both public and private sector services.

- The Ministry of Economic Affairs and Digital Transformation and Ministry for Home Affairs steers the strategic direction of and vision for digital identity.
- There is a single supervisor body the Ministry of Economic Affairs and Digital Transformation for the trust service providers issuing qualified certificates (allowed to use for access public services). The responsibility of the issuing of the DNIe is assigned to the Ministry for Home Affairs through the National Police General Directorate (DGP)
- DNIe is funded by public funding
- European standards, eIDAs Regulation. There eIDAS supervisory body for the trust service providers assess the conformity of qualified services providers according to eIDAS Regulation and its implementing acts by means of an administrative procedure. The trust service providers are obliged to send to the SB a conformity assessment report issued by a conformity assessment body, according to eIDAS Regulation.
- eIDs based on qualified electronic certificates issued by service providers (public or private) included in the trusted lists of qualified trust service providers required by the Regulation (EC) No 910/2014/EU(eIDAS), as those included in the *Documento Nacional de Identidad electrónico* (DNIe-electronic National Identity Document www.dnielectronico.es) or other means like systems based on keys.
- For public sector, there is an eID gateway called *Cl@ve* that is a common platform for identification and authentication. This system means Public Administrations do not need to implement and

[41]Notification Form for Electronic Identity Scheme under Article 9(5) of Regulation EU 910/2014, Official Journal of the European Union, pp.9: https://ec.europa.eu/cefdigital/wiki/display/EIDCOMMUNITY/Spain?preview=/62885675/65972507/Notificacion%20DNIe_2015_1984_EN%20(6).pdf

manage their own identification and signature systems. Equally, citizens do not have to use their own identification methods to interact electronically with the Administration. This gateway allows the use of identification systems based on keys (username and password systems) as well as electronic certificates (including the DNIe). (https://clave.gob.es/)

- In May 2021, a Ministerial Order was issued regulating remote identification by video identification methods for issuing qualified certificates. The trust service providers are now starting to implement the methods. National Identification Document, issued by National Police Department (Ministry for Home Affairs)

Technical choices

The different means for authentication used in Spain include smartcards; digital certificate files; and two factor authentication (2FA) that confirms access to a mobile phone number

Portable (cross-platform, cross-sectoral, cross-border) digital identity

- **Cross-platform:** The Spanish eID is not available through mobile devices.
- **Cross-sectoral:** In Spain, private service providers can use DNIe for service user authentication and verification.
- **Cross-border:** Governed and made possible by the EU eIDAS Regulation. Currently the national eID from 13 other EU Member States can be used for authentication and verification in order to access public sector services in Spain: Germany, Italy, Luxembourg, Estonia, Croatia, Belgium, Portugal, Netherlands, Czech Republic, Latvia, Slovakia, Denmark, Lithuania. The eIDAS Regulation and GDPR determines the extent to which privacy protection and data security approaches of other countries are consistent with Spain's policies when agreeing on mutual recognition.

Data visibility and citizen consents

In Spain, citizens have a legal right to opt out of the use of Digital Identity

The European GDPR (Regulation (EU) 2016/679, General Data Protection Regulation) and National Law on data protection and digital rights (*Ley Orgánica 3/2018, de Protección de Datos Personales y garantía de los derechos digitales*). eIDAS Regulation establishes security requirements for eID systems and for trust services providers. GDPR is also of application to the providers and establishes the security measures for data protection.

The Data Protection Authority (DPA) is not specifically targeted at Digital Identity but provides an oversight function.

Citizens are proactively informed by authorities about any processing of their personally identifiable data and can provide and revoke consent for the re-use and sharing of attributes or data originating from their Digital Identity

3. Uptake and adoption of Digital Identity

In Spain, it is mandatory for public sector organisations to use the eID for user authentication and verification. For public sector, there is an eID gateway called *Cl@ve* that is a common platform for identification and authentication. This system that prevents Public Administrations from having to implement and manage their own identification and signature systems, and citizens having to use different identification methods to interact electronically with the Administration. This gateway allows the use of identification systems based on keys (username and password systems) as well as electronic certificates (including the DNIe). (https://clave.gob.es/) Resources such as integration packages are available and

there is support to help the public sector teams. 100% of public sector services where it would be necessary to authenticate users are using the eID. eID is used to access or consume public sector services 350 million times per year.

During lock-down, one lesson learnt was the need to have a remote identification system to issue qualified certificates in order that the citizens can access public services without the need of physical presence. We put in place a transitional measure for this purpose during the state of alarm in March and June 2020, and recently in May 2021 a Ministerial Order establishing the requirements for video identification has been adopted.

4. Ongoing and future Digital Identity reforms

A pilot of Self-Sovereign Identity (SSI) is foreseen within the framework of the European Blockchain Services Infrastructure (EBSI) working group of the European Commission. Spain considers that governments in a SSI system should have the role and power to provide the identity to all the citizens. It is the only way to ensure that the person acquiring the digital identity is really who claims to be. That should be the basis of the system, but also that governments should regulate and supervise the providers of identities and attributes, and monitor compliance with data privacy and respect of fundamental rights of the citizens.

Spain will observe developments under the EU proposal for a Regulation on digital identity.

Turkey

1. National context

The national digital identity system in Turkey used for accessing public sector services is provided through the e-Government Gateway. The digital identity system is available to:

- citizens of the Republic of Turkey, who are over the age of 15,
- blue card holders
- foreigners, with a photographic identity card (identity card, marriage certificate, passport and driver's license, lawyer identity card, blue card, residence permit, judge and prosecutor identity cards, valid work permit card)

Individuals obtain their e-Government Gateway passwords in person or through a power of attorney from PTT (Turkish Post) offices, central directorates, or authorized branches. Persons who have been appointed as guardians by a court decision can obtain an e-Government Gateway password through their guardians.

Turkey's total population in 2021 was 83.6 million, and the total eligible population for digital identity based on age was therefore 64.5 million, or 77% of the total population.

2. Current national Digital Identity management system

The country model

The model for digital identity system in Turkey is sector specific with reusable public sector digital identity. This implies that there are private sector managed digital identity systems for accessing private sector services and a public sector managed digital identity system for accessing both public and private sector services.

- The task of establishing and managing the e-Government Gateway is assigned to the Presidency Digital Transformation Office, and the development and operation of the system are carried out by

Türksat Company (*Türksat Uydu Haberleşme Kablo TV ve İşletme A.Ş.*). The PTT General Directorate (Turkish Post) provides citizens with the Digital Turkey passwords as the institution with the most widespread distribution network throughout the country.

- The Turkish government collaborates with mobile operators (Türksat), banks and financial services providers, and software companies for the development and operation of the national digital identity system. Identity providers in Turkey are financed by the government and financial institutions.
- The following identity standards exist in Turkey:
  - eİDAS and standards related to eİDAS Plus
  - Standards for the application of identity cards: ICAO 9303, ISO/IEC 14443, ISO/IEC 7810, ISO/IEC 7816, TS 13678, TS 13679, TS 13680, TS 13681, TS 13582, TS 13583, TS 13584, TS 13585, PCI.
- In Turkey, it is not possible for citizens to obtain their e-Government Gateway password through an online-only process. Face-to-face authentication is a part of secure password applications. Citizens over the age of 65 and who have not received a password before have the right to apply for delivery to their home address. The process for obtaining a digital identity is:
  - The individual submits their identity number and photo containing ID to the PTT (Turkish Post) central directorates or authorized branches. Alternatively, the password can be obtained from the PTT branches through the power of attorney or the guardianship document provided by the relevant judicial units. The password can also be obtained from Embassies and Consulates abroad.
  - Another option is that if an individual logs into the e-Government Gateway using a mobile signature, electronic signature or internet banking, the password can be created directly on the portal but requires the user to be able to authenticate themselves through the other means. Individuals can also log in to the system with an electronic ID card and then create a password.

Technical choices

The different means for authentication used in Turkey include smartcards; digital certificate files; e-signatures; username and password; and two factor authentication (2FA) that confirms access to email account, mobile phone number, or mobile device.

Turkey's digital identity is based on Public Key Infrastructure (PKI) and One Time Password (OTP). Blockchain-based digital identity will be available soon.

Turkey reports that user privacy has been well protected during the COVID-19 pandemic. Türksat, that runs the e-Government Gateway, holds the ISO 27001 information security management system certificate and undergoes regular audits. In addition, security and penetration tests are conducted by independent security companies for the e-Government Gateway. All information presented on the e-Government Gateway is instantly obtained from the relevant institutions, compiled and presented to citizens. The e-Government Gateway only authenticates citizens and receives the information from the systems of the institution that owns the data over secure communication networks. Each citizen can only access their own information.

All of the information about the services accessible through the e-Government Gateway is provided by the relevant public institution. Data traffic between institutions and e-Government Gateway systems is protected at the highest possible level since the information is not stored in the e-Government Gateway systems but displayed instantly from institutions. The entire system is monitored on a 7/24 basis and responds promptly to all extraordinary events.

Portable (cross-platform, cross-sectoral, cross-border) digital identity

- **Cross-platform:** The national digital identity of Turkey can be accessed via different mobile devices.
- **Cross-sectoral:** The e-Government Gateway digital identity passwords are only used for accessing public services. However, as the e-Government Gateway authentication platform allows individuals to authenticate themselves via the authentication platforms of several banks, the banking digital identity solutions in Turkey are considered cross-sectoral.
- **Cross-border:** No other country digital identity is recognised for service user authentication or verification in Turkey.

Data visibility and citizen consents

In Turkey, citizens have a legal right to opt out of the use of digital identity. There are no public services that cannot be accessed by individuals that exercise this right.

In Turkey, The Law on the Protection of Personal Data No. 6698 was published in the Official Gazette on 7 April 2016 and 29677 numbered entered into force. Turkish Data Protection Authority was established under the same Law. In Turkey the Human Rights and Equality Institution of Turkey, affiliated to the Ministry of Justice, with public legal entity status and administrative and financial autonomy, established by law No. 6701 based on the international law monitors and oversees the impact of digital Identity on individual privacy and freedoms. The authority is not independent but has offsite and onsite investigatory power and sanctioning power.

In Turkey, personal data may be processed only in cases where one of the following conditions is met:

- The data subject has given his/her explicit consent.
- It is expressly provided for by the laws.
- It is necessary for the protection of life or physical integrity of the person himself/ herself or of any other person, who is unable to explain his/her consent due to the physical disability or whose consent is not deemed legally valid.
- Processing of personal data of the parties of a contract is necessary if it is directly related to the establishment or performance of the contract.
- It is necessary for compliance with a legal obligation to which the data controller is subject.
- Personal data being made public by the data subject himself/herself.
- Data processing is necessary for the establishment, exercise or protection of any right.
- Processing of data is necessary for the legitimate interests pursued by the controller, provided that this processing does not violate the fundamental rights and freedoms of the data subject.

Pursuant to Article 4, Personal data shall only be processed in compliance with procedures and principles laid down in Personal Data Protection Law or other laws. The following principles shall be complied with while processing of personal data:

- Lawfulness and fairness
- Being accurate and kept up to date where necessary.
- Being processed for specified, explicit and legitimate purposes.
- Being relevant, limited and proportionate to the purposes for which they are processed.
- Being stored for the period laid down by relevant legislation or required for the purpose for which the personal data are processed.

Natural persons whose personal data are processed have right to request to data controllers within the scope of their rights specified in Article 11 of the Law. This right consists of the followings:

a) to learn whether his/her personal data are processed or not,
b) to demand for information as to his/her personal data have been processed,
c) to learn the purpose processing of his/her data and whether these personal data are used in compliance with the purpose,
d) to know the third parties to whom his personal data are transferred in country or abroad,
e) to request the rectification of the incomplete or inaccurate data, if any,
f) to request the erasure or destruction of his/her personal data under the conditions referred to in Article 7,
g) to request reporting of the operations carried out in compliance with sub-paragraphs (d) and e) to third parties to whom his personal data have been transferred,
h) to object to the occurrence of a result against the person himself/herself by analyzing the processed data solely through automated systems,
i) to claim compensation for the damage arising from the unlawful processing of his/her personal data.

Data subjects shall make a request to data controllers within the scope of their rights specified in Article 11 of the Law, in writing or by registered electronic mail (KEP) address, secured electronic signature, mobile signature or by the e-mail address which has been previously entered into the data controllers' system or through a software or application designed for purposes of this request. The data controller is obliged to take necessary organizational and technical measures to conclude the requests to be made by data subject within the scope of the Communiqué, effectively and complying with norms of lawfulness and fairness. Data controller shall act on the requests or refuses them together with justified grounds. Data controller shall communicate its response to the data subject in writing or by electronic means Data controllers shall conclude the demands in the request within the shortest time by taking into account the nature of the demand and at the latest within thirty days and free of charge. However, if process requires additional costs, fees may be charged in the tariff specified in Article 7 of the Communiqué. If the request is caused due to the fault of the data controller, the fee is refunded to data subject.

Laws and mechanisms in Turkey to ensure the security of user data in private sector identity solutions and that private sector actors cannot commercialise data obtained from digital identities without a user's consent include the Turkish Personal Data Protection Legislation, regular audits by the Personal Data Protection Authority, Banking Law No. 5411 and sub-regulations.

3. Uptake and adoption of Digital Identity

The use of digital identity for service user authentication and verification is mandatory for public sector organisations in Turkey. As a result, 50%-74% of public services where it is necessary to authenticate users are using the available digital identity solutions. The remaining services are carried out in traditional, administrative ways. On average, individuals use the available digital identity solution to access or consume any public sector service 43 times per year. The government has different mechanisms in place to provide technical and financial support to public sector teams implementing the digital identity solutions.

In December 2019, prior to the COVID-19 pandemic outbreak, the number of individuals with a digital identity was 45 million. The percentage of the eligible population that had a digital identity was therefore 70%. In April 2021, a year after the first wave of the pandemic, the total population with an active access to a digital identity was 54 million, meaning digital identity adoption had increased by 21% reaching 84% of the eligible population.

During the COVID-19 pandemic Turkey pursued an inclusive approach when it comes to informal and formal employed or unemployed population, for the disabled, and for the elderly population. To fulfil the social distancing measures during the pandemic more than 500 government digital services were provided to citizens and more than 300 services to businesses. Digital identity enabled the authentication and access to these services. Services that benefitted the most from the possibility of digital identity authentication during the pandemic include pandemic social support applications and HES (HES (*Hayat Eve Sığar* – Life Fits Into Home) code generation and listing.

4. Ongoing and future Digital Identity reforms

In terms of lessons learned from their digital identity reforms, Turkey finds online education, remote working and e-commerce as inevitable technology infrastructures that force and promote the adoption of blockchain-based solutions into daily life. In line with this, Turkey is working on providing blockchain-based digital identity solutions in the future.

United Kingdom

1. National context

GOV.UK Verify is a digital identity system operated by the public sector but delivered by private sector identity providers, and used for authentication purposes by public sector services.

In the United Kingdom, all individuals above 18 years old can request a digital identity. The total population of the country in 2021 was 66.6 million, with the total population eligible for a digital identity (based on age) 52.7 million, or 79% of the total population.

2. Current national Digital Identity management system

The country model

The Government Digital Services (GDS) within the Cabinet Office steers the strategic vision for and direction of digital identity verification for public sector services. The Department for Digital, Culture, Media and Sports (DCMS) steers the strategic vision for digital identity verification when it comes to the private sector. GDS is in charge of delivering GOV.UK Verify which is the digital identity system for accessing public services. Identity Providers in the UK are funded privately.

The Good Practice Guide 45 provides guidance to service providers on how to prove and verify someone's identity - not limited to digital identity verification. The guidance aligns with the following international standards and regulations:

- Digital ID and Authentication Council of Canada (DIACC) Pan Canadian Trust Framework Model
- the EU electronic identification and trust services (eIDAS) regulation
- ISO/IEC 29115
- NIST 800-63

In order to connect identification records across services, there is no single national identification number but various other mechanisms, including the national insurance number. Citizens can obtain a digital identity through GOV.UK Verify online. The process is:

- Choose option to verify identity online
- Choose identity provider
- ID provider requests data to confirm identity

- If successful user returns to service for access

Technical choices

The means available to use for authentication through GOV.UK Verify are two-factor authentication that confirms access to a mobile phone number or an email account. There are no available figures on the number of authentications issued through these means.

Portable (cross-platform, cross-sectoral, cross-border) digital identity

- **Cross-platform:** GOV.UK Verify can be accessed through a mobile device, and is not device specific.
- **Cross-sectoral:** GOV.UK Verify can only be used to access public sector services.
- **Cross-border:** The UK does not recognize GOV.UK Verify. All EU countries that have notified under EU eIDAS Regulation can use their digital identity to access non-public sector services. Under the UK GDPR and adequacy determination would be required to assess the data protection and security approaches of another country before agreeing mutual recognition on digital identity.

Data visibility and citizen consents

The UK General Data Protection Regulation ensures the protection of privacy in digital identity systems and the legitimate and proportionate processing of a citizen's identifiable data through digital identity systems.

Citizens are proactively informed about the processing of their personal identifiable data through privacy notices via email. Users of GOV.UK Verify can access and see what attributes about them are being shared and re-used, and with whom, and they are also able to both provide and revoke consent. Furthermore, civil society organisations in the country are monitoring the process by which personable identifiable data are being shared and re-used.

3. Uptake and adoption of Digital Identity

The use of GOV.UK Verify for user authentication and verification is not mandatory for public sector organisations. There are no available figures on the update and adoption of GOV.UK Verify for service providers.

In December 2019, prior to the COVID-19 pandemic outbreak, the number of individuals with a digital identity was 5.6 million. The percentage of the eligible population that had a digital identity was therefore 11%. In April 2021, a year after the first wave of the pandemic, the total population with an active access to a digital identity was 8.4 million, meaning the share of eligible population with a digital identity had increased by 5 percentage points to 16%.

4. Ongoing and future Digital Identity reforms

The United Kingdom's Government's response to the Call for Evidence on Digital Identity on 01 September 2020 committed to promoting an enabling market of digital identity standards. The Government published an alpha of the UK digital identity and attributes Trust Framework on Thursday 11 February 2021. The trust framework is a set of rules and standards which organisations agree to follow. If an organisation is part of the digital identity trust framework, then you will know they follow agreed requirements which safeguard data and protect privacy. The alpha contains rules on privacy and data protection, fraud management, security, and making sure products and services are inclusive. The trust framework is being published as an alpha (prototype) so that DCMS can test it with services, industries, organisations and

potential users. DCMS are taking this collaborative approach to make sure that when the final version is published it meets the needs of those who will rely on it. The next version of the trust framework alpha is due to be published in the summer. It will include information about the certification process by which organisations will be assessed to gain a Trustmark.

DCMS is also preparing to consult on digital identity legislation during this year. This will include proposals for a governing body to own and manage the trust framework to build public and industry confidence in this new market. A priority for the United Kingdom is making sure that framework is aligned with the approach taken by other countries. There are clear benefits from achieving international interoperability, reducing fraud and trade frictions, and offering increased choice and security for individuals and businesses that want to prove identities across international borders.

United States of America

The United States government has a system of federated identities. Identities are generated at the local government level and used to create state government level identity credentials.

At the federal government level, the United States government is working to recognize identities from the state and local levels to enable secure digital access to federal services while prioritizing privacy, minimizing data collection, and ensuring user consent before their data is used or shared. This includes firewalling to ensure that data is not shared with agencies who do not need access to the data to provide the service requested, as well as a user-friendly format that does not require data collection for the provision of services that do not require such data.

The United States considers that the centralization of identity information brings with it inherent risk, particularly related to user privacy; whereas, federation enables easy and secure exchange of information between ecosystems.