



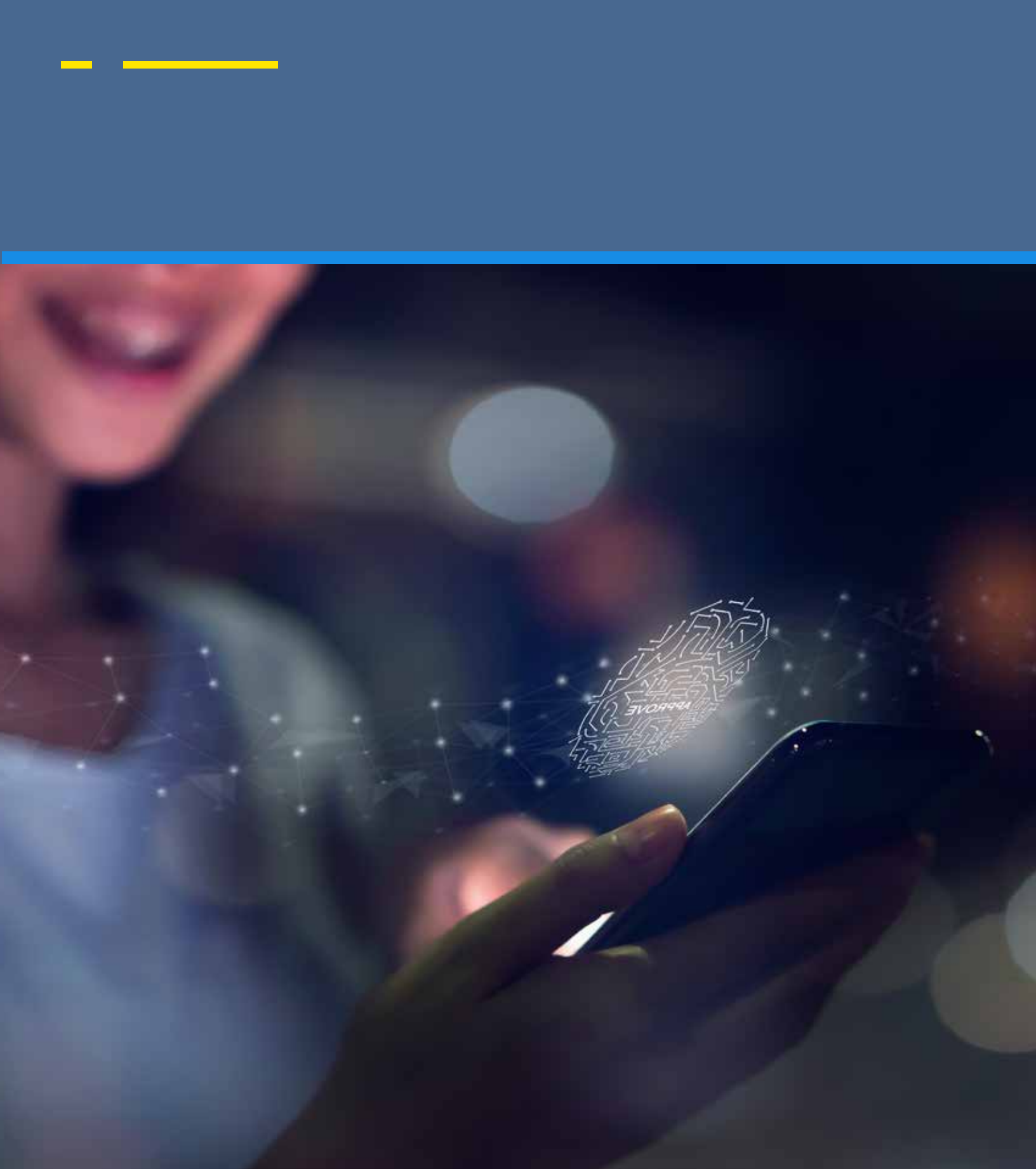
**Universal Digital Identity  
Policy Principles to  
Maximize Benefits  
for People: a shared  
European and Canadian  
perspective**

**Human belonging in a digital world**

DIACC  CCIAN



HUMAN TECHNOLOGY  
FOUNDATION





# Introduction

---

**As we approach the quarter-mark of the 21st Century, there is general agreement among policymakers and people around the world that the establishment of a strong, reliable, privacy-respecting, and principle-driven ecosystem to verify and authenticate identity (ID) has become more important than ever.**

Digital identity and authentication infrastructure has the capacity to protect data, empower people, and help both public and private sector organizations provide services and information more effectively. As the pandemic has shown, being able to rely on a digital identity ecosystem of solutions and services that safeguard data, maximize peoples' options and help organizations provide services rapidly can be invaluable in times of crisis as well as times of stability. Our social safety net is increasingly dependent on our ability to rapidly deploy social services and economic benefits using secure, reliable digital credentials. Moreover, enabling digital identity is arguably a prerequisite for developing a more human-centred internet and to unlocking the “promise” of emerging technologies such as “Web3”.

One study by the Digital ID & Authentication Council of Canada (DIACC) asserted that, by working together to advance policy and technology design principles that put people - their benefits, their needs, and their concerns – at the center, nations have the opportunity to gain between 3% and 13% of unrealized GDP potential, as further supported by a McKinsey study. Both studies estimated the potential value to be gained by reducing fraud, creating efficiencies, and enabling new services and businesses with capabilities not currently using traditional methods of identification.

As with every innovative opportunity, progress must come through collaborative action balanced with pragmatism and transparent protections set out in policies that guide technology for the good of humanity.



## Our Goal

---

**The optimal development and implementation of digital identity related policies are the focus of this joint project by DIACC, a Canadian non-profit coalition of private and public sector organizations that collaborate to define and certify a duty of care for identity related services, and the Human Technology Foundation (HTF). HTF is a network with several thousand members that operates in Paris, Montreal and Geneva, and with the intention of placing the human being at the heart of technology development and putting technology back at the centre of social debates.**

In support of advancing the practical application of digital identity technologies, this paper has been developed to help policy-makers define policy design principles that support a common duty of care for organizations that implement digital identification systems and to help to enable them to consistently apply that duty of care.

This paper has been written with human considerations at the center, to inform policy makers and influencers from the public and private sectors, as well as the general public that may have interest in policy design.

Below, we highlight some of the latest research, analysis and lessons learned related to the ongoing development of governments' digital identity strategies. We do so recognizing that governments and private sector entities must deeply engage in fast-reacting and smart policy-making to secure and protect data related to people and organizations. Extensive public engagement is also needed to inform digital transformation and promote inclusive and equitable solutions that underpin trust in digital ecosystems as the digital economy continually develops and expands.

DIACC and HTF hope decision-makers in national and sub-national governments, along with private sector entities, will use the information herein as a tool to work urgently with all stakeholders to establish inclusive, privacy-protecting, and trustworthy digital identity related policies that empower individuals, businesses, the public sector, and civil society.

Digital identity encompasses complex concepts and underlying technology, and is often difficult to understand (as are the digital ecosystems in which identity is a common underlying thread). To help further clarity of understanding, and to anchor policy recommendations in considerations common across international populations, we make use here of research-based scenarios to narrate concepts and principles in human terms, while focusing on human-centered policy and principles to guide frameworks for identity in society, rather than delving into solutions, standards or specific techniques to implement digital identity.



# What is Digital Identity

---

## An extension of you

Digital identity is an evolution of current systems that are used to establish and confirm identity in an ever-expanding range of contexts. As a means of identifying a person securely during on and offline interactions, digital identity functions as an extension of existing physical identity documents such as passports, driver's licenses, and bank cards. At its simplest level, digital identity is a manner of accurately and securely representing who you are.

Use cases for digital identity might include:


- Producing an authentic birth certificate or driver's license
- On-boarding a person to a digital service
- Protecting children from adult content
- Signing a business contract
- Opening a bank account
- Filing a tax return
- Applying for university or college admission
- Claiming a medical prescription
- Proving age of consent
- Renting a car and proving the ability to drive
- Checking into a hotel
- Identity verification
- Sharing general interest data for public use
- Enhancing political interaction and/or voting
- Boarding a plane
- Crossing a border

## Much more than basic credentials

Current identity cards with official and mandatory data are used to identify its holder and offer some security, but they have significant shortcomings. The data associated with current identity documents are not portable, are fragmented, and are outside the control of the cardholder.

Digital identity goes beyond the basic authentication functions covered by traditional documents attesting to the identity of individuals or companies. Unlike a traditional identity card, which by its nature is unchangeable and limited in its content, a digital identity credential allows the addition of new information, is potentially compartmentalized, and can employ various levels of security.





One's digital identity credential can be stored in a digital wallet, or used in an identity network, allowing the storage and use of identity data and various attributes/credentials, based on common standards, under the sole control of the user.

## Building Trust

Policy that solves people's problems while maintaining a balance of intuitive control, protection, and precaution can help to build societal trust. This requires a more general awareness among users regarding the potential of their data.

Digital identity tools and services can help governments and businesses to build trust through secure, privacy-respecting and authenticated engagement. Public and private sector entities can demonstrate their commitment to empowering and protecting people by designing solutions and services following people-centered policy guidance. While technology offers many evolving capabilities, technology alone can not solve all challenges related to a lack of trust.

## Addressing the public interest

Various studies have found substantial public support for advancing digital credentials. For instance, a recent DIACC survey found that 78% Canadian respondents believe it is very important or somewhat important that the Canadian government move quickly to enable a safe and secure digital identity for the whole country. And two-thirds of Canadian respondents say the pandemic has made it more important to have a secure, trusted, privacy-enhancing digital identity to help Canadians transact safely and securely online. The survey also found that a strong majority of Canadian respondents agree that they should have access to the personal data collected about them by federal and provincial governments and private companies.

Similarly, the European government Eurobarometer survey found that 72% of users want to know how their data is processed when they use social media accounts. 63% of EU citizens want a secure single digital identity for all online services.

On a global scale, the 2021 EY IPSOS MORI study said there is a broad appetite among citizens for more digitally enabled public services and, while many want to have more of a say in how they should be delivered, people don't all perceive digital identity in the same way.

However, the EY IPSOS MORI study also found that a significant minority of citizens lack the skills or tools to access digital services. The challenge for the government is to work with individuals to harness and control data to become more efficient and effective without disadvantaged groups being left further back.

The benefits of these innovative digital systems are not guaranteed, offering numerous immediate and ongoing hurdles for policymakers and governments.



## Action urgently needed

Action is urgently needed and policy makers should explore opportunities to observe and participate in digital identity related proof of concepts, pilots and other projects to gain “hands-on” experience that will inform policy development supported by people-centered design principles.

The risks of not moving ahead with the policy design needed to support transformation will include loss of strategic positioning on a global scale, worsening cyber security attacks, and failure to realize substantial economic growth potential. Governments and the private sector risk falling behind jurisdictions that are prioritizing person-centered digital identity. Lack of coordination between public and private actors could raise serious questions about sovereignty.

Conversely, establishing digital identity that adheres to defined policy principles not only helps foster trust amongst citizens and consumers, it also helps public and private sector organizations to ensure their duty of care has been addressed. Well-designed credentials can empower individuals with more privacy and greater control of data protection and sharing. Entities that adopt and implement best practices or frameworks that help to define an expected duty of care will demonstrate an investment in risk mitigation that may also protect them from certain liabilities.

A strong and secure digital identity ecosystem of tools and services based on universal principles can dynamically advance a wide range of civic, social and economic priorities. It can better support democratic, civic, and social engagement by connecting governments to authenticated citizens and residents needing prompt support and information while greatly improving service delivery. It can also promote opportunities for data altruism enabling people to donate medical data, for example, that might help to identify treatments and cures to medical conditions. And it can reduce costs for governments, consumers, and businesses, and drive GDP growth.

# One size doesn't fit all

One of the important lessons learned over the past several years as technology has become ever-more embedded in our lives, is that individuals have very different views as to the impact of such technology on their lives and as to whether (and under what circumstances) technology increases or decreases their well-being.

In short, if “it’s all about trust”, then it’s also fair to say such trust must be earned. Depending on one’s background and one’s beliefs, the factors that will establish a trusted relationship with a technological solution will vary greatly.

To assess the overall landscape for digitalization and examine the impact that the principles enumerated below will have on different groups within society, this report uses representatives of four groups of people identified by a 2021 EY/IPSOS MORI global study entitled “How can digital government connect citizens without leaving the disconnected behind?”

*The four groups – Capable Achievers, Struggling Providers, Privacy Defenders, and Tech Skeptics – represent important segments of the population categorized in EY’s global research. Below we look at each group and their digital needs and issues.*



**Catherine is a Capable Achiever:** *Independent, successful, and satisfied with their life, Capable Achievers are pragmatic technophiles who embrace digital innovation. They trust governments to use their data appropriately, but worry about it getting into the wrong hands.*

Catherine is 54 and lives with her husband in their own house in the suburbs. With two children at university, she enjoys a comfortable life, thanks to her job as an executive in a global media company. Catherine feels satisfied and is optimistic about her future. She owns and uses a smartphone and laptop daily for work, keeping in touch with friends and family, following news, streaming her favorite shows, shopping online and managing finances. She views technology as a positive force that makes tasks easier. But, she has yet to buy any smart appliances or wearables. Catherine prioritizes speed and convenience when she interacts with public services – which she does primarily for health and administrative tasks. She doesn’t like to submit her personal details every time she accesses a government website, and would prefer having a single portal, a unique digital citizen identity and log-in for convenience.



**Jonathan is a Struggling Provider:** *Struggling Providers are younger, tend to be in low-paid, less secure work, and are above-average users of welfare services. They are ambivalent toward technology, lacking the access and skills for it to make a big difference to their lives.*

Age 34, with a wife and two daughters, Jonathan lives in the city, where he works with a courier company. He has a health condition that restricts his ability to do different kinds of work. His wife stays at home to watch the children and her elderly father, who lives with them. The family relies on Jonathan’s income. With no sick pay, pension or other company benefits, and no guarantee of regular work, he is anxious about the future. The family relies on public services, but Jonathan thinks the government has little understanding of his family’s circumstances and the support he gets is not enough. Jonathan lacks confidence and skills to use technology. He has a pay-as-you-go smartphone and a reconditioned laptop, but can’t afford high-speed internet. He has little faith that modern technology will make life better. He would prefer to interact with government or public service providers by phone or email rather than through a website – though he is open to using social media. He would welcome a single government portal through which to access all services – if only he was able to connect with it. He’s fairly ambivalent about the government sharing his personal data, either internally or with private companies.





**David is a Privacy Defender:** *Privacy Defenders tend to be older, independent and financially comfortable. They value technology and the benefits it provides to them, but are extremely cautious when it comes to sharing their personal data with government or private companies.*


David is 48, lives with his wife and was happy with his life before the pandemic, but now feels aware of the need to keep his skills up to date in case he needs a new job. When David interacts with government services, he is rarely satisfied. He's frustrated with the inefficiency of accessing services and would like better, faster, easier interactions and more knowledgeable staff to treat him with respect. David has a strong awareness of his digital footprint and is cautious when sharing his personal data. Privacy and anonymity are core priorities. He distrusts social media and shares minimal personal information on networking sites. Although he would like services to be more personalized to meet his individual needs, he limits how much data he shares with government agencies and private sector companies. David is uncomfortable at the prospect of the government sharing his data within or outside of the public sector, even when this would help planning and decision-making that would directly benefit citizens. Although he gets impatient at having to repeat his personal details when interacting with government agencies, he still prefers this to having a digital citizen ID that would allow different organizations to access his personal data. Until he is reassured that his data is completely safe, he doesn't want to see any advanced digital solutions in public services.



**Christine is a Tech Skeptic:** *Older, on lower incomes and relatively dissatisfied with their lives, Tech Skeptics are distrustful of the government and skeptical about the benefits of technology. They tend to be opposed to data sharing, even if there is a clear purpose.*

Christine is a widow with grown-up children, and will soon retire from her job in the human resources department of a logistics company. She is concerned about financial security: her pension plans were damaged by the financial crisis over a decade ago and have yet to recover. She is skeptical about the benefits of technology, viewing it as something that works to the advantage of the rich and powerful, rather than ordinary citizens. Despite this, she owns a smartphone, laptop and TV, which she uses for limited tasks such as keeping in touch with friends and family, and shopping. She sees little point in improving her digital skills and is not convinced that technological innovation is key to meeting the economic and social challenges that the world faces. Although Christine would like it to be easier to access services, she is against single digital citizen IDs, especially if these were to be linked with personal details relating to income. She is a strong opponent of government sharing her personal data – either internally or with private companies – even where there is a clear purpose, such as combatting criminal activity or terrorism. She thinks any benefits of data sharing would be canceled out by the threat to her privacy and security. She is also wary of sharing personal information with businesses when she performs transactions.

**When designing policy it must be understood that not all people perceive digital identity in the same way. Therefore working with diverse personae such as Catherine, David, Christine and Jonathan can help to identify similarities and differences in the perceptions of people and, ultimately, to build trust and consensus through the adoption of core principles that serve to address their concerns.**



# The risks and benefits of digital identity deployment

---

## Managing risks to maximize benefits

---

**Being able to call on a digital identity ecosystem that protects data, empowers people to access both public and private sector services and helps organizations to provide such services more effectively is invaluable.**

For the world's innumerable small and medium-sized businesses, the savings in procurement, access to financial services, and other operations from a digital identity system could add many billions of dollars in value and investments annually. As well, in the global financial sector, operational efficiencies created by reducing manual processing costs and curbing fraud would provide substantial benefits for consumers and businesses.

This innovation can also empower citizens with the digital credentials necessary to access, manage, and share their own data, ensuring people have control over the important information they need to manage their health, businesses, and digital services.

As with any new technology, there are risks associated with the implementation of digital identity policies and they are not insignificant.

However, as this paper hopes to demonstrate, a well-designed and appropriately governed implementation of digital identity can serve to amplify the benefits and mitigate the risk.

### **Interoperability, efficiency and automation**

When a person shows a physical identification card, the data in that card is static. It cannot flow automatically to or from the entity verifying it. It cannot automatically populate forms or automatically be verified for authenticity.

By contrast, digital identity facilitates all of these features. For example, digital identity can be used in a health services setting to facilitate the transfer of medical files from a hospital to a patient's physician. Or, using digital identity, an individual can automatically complete fields of a form, unlock access to previously submitted information, or validate external credentials.

CATHERINE

*I used my digital identity to sign a new supplier agreement - it not only proved who I was but also confirmed that I was a legitimate member of our professional association.*



## Data minimization

When using traditional means of identification, people often share more information than required for the transaction. By contrast, digital identity credentials have the ability to allow individuals to choose to share only the minimum information necessary for the specific context. The decompartmentalization of identity data helps (if so desired) to preserve a person’s anonymity.

This principle could be implemented for the protection of minors online, for example. In fact, effective protection of minors online requires their identification and the supervision of their access to online services and content. The implementation of data minimization is providing everyone with the ability to issue only proof of a single attribute (proof of majority, proof of residence, proof of diploma, etc.) without revealing the other elements that constitute an identity. Data Minimization provides an answer for identifying users’ age while preserving privacy.

DAVID

*I was glad to learn that if my kid’s identity gets checked to buy alcohol, they are able to prove they are of legal drinking age with a digital identity credential, instead of using a piece of identification that has their name, address, birth date and other personal information on it.*



## Modularity

Unlike a traditional physical credential identity card, a digital wallet that contains one’s identity credentials allows the individual to manage information and to add (or remove) associated digital credentials.

For example, as a person makes their way through university, they might choose to associate a variety of new credentials to their digital identity that they could then chose to use in a variety of contexts such as “voting age, eligible to vote”, “age of majority, eligible to purchase alcohol”, “full-time student, eligible for employment”.

The fact that such credentials may be relevant to a variety of services and that they may be of varying degrees of sensitivity helps to explain why such credentials must be compartmentalized and subject to various levels of security.



## Inclusion

### Case study: India's Aadhaar

---

For over 1 billion individuals worldwide, their lack of recognized identification bars them from having access to basic goods and services, according to the United Nations study “Roadmap for Digital Cooperation”. The study found that “a ‘good’ digital identity that preserves people’s privacy and control over their information can empower them to gain access to much-needed services.” Initiatives such as Identification for Development and the United Nations Legal Identity Task Force can help countries realize the transformative potential of digital identification systems.

India created the world’s largest voluntary biometric identity system using faceprints, face and eye scan. Aadhaar, meaning “foundation,” was put in place in 2009 as a centralized application to allow every resident of the country to easily establish their identity. By late 2021, the Unique Identification Authority of India reported that 1.3 billion people, or roughly 99% of Indian adults, had enrolled in Aadhaar.

The program improved financial inclusiveness by opening up access to bank accounts and service delivery by facilitating transfer of government support funds to beneficiaries. The program is credited with providing key infrastructure for food and financial distribution that helped keep extreme poverty at pre-pandemic levels during COVID-19. India’s 2019 “State of Aadhaar Report”, which surveyed 167,000 users, found that 92% of respondents were satisfied with how the system worked. The results are an indication of the power that digital identity can have when harnessed for social good.

## Democratic and social engagement

### Case study: Estonia's I-voting system

---

Estonia has used digital identification to enable online voting since 2005. Nearly half of Estonian voters used “I-voting” to vote during the last European Parliament elections in 2019. In the wake of the COVID-19 pandemic, the Estonian system has proven to be not only convenient but also a valuable tool to support public health measures. The Estonian I-voting system allows people to exercise their democratic rights without putting public health at risk.

## Facilitation of data altruism

### Case Study: Barcelona's Salus.Coop

---

The Human Technology Foundation explored the concept of Data Altruism. According to the EU Data Governance Act, which was adopted in May 2022, data altruism is the voluntary sharing of data based on consent or permissions for purposes of general interest such as healthcare, combating climate change or improving public services. This innovative system distinguishes itself from the two main existing data sharing systems: the commercial system (in which data is processed in a competitive market) and the open data system (in which certain types data sharing is rendered compulsory by law). Data altruism innovation is enabled by the creation of organizations that are altruistic regarding data. These new actors must be trusted, independent, non-profit third parties ensuring the full transparency of data gathering and sharing for public interest purposes. It found a compelling example in the work carried out by Javier Creus, who created "Salus.Coop" in Barcelona, a non-profit citizen data cooperative for health research that facilitates the sharing by users of their health data for medical research purposes.

Developments of such scale that serve the public interest are only possible through mass processing of health data. Digital identity could contribute to initiating a social movement that makes data sharing for the public good a social norm.



## Surveillance and lack of accountability

There is considerable public concern in many countries about the impact and potential risks of digital verification systems – fears that have grown as the COVID-19 pandemic rapidly increased the expansion of internet-based activity and service delivery. That governments might abuse the digital identity verification capabilities by gaining undue access to personal data typically tops the list of concerns.

These fears are not merely theoretical. In 2017, for example, a report by the Center for Internet and Society analyzed publicly available datasets associated with Aadhaar and found that 100-135 million Aadhaar identifying numbers and 100 million bank account numbers had been disclosed.

CHRISTINE

*In theory I'd like public services to be easier to access, and I definitely want to minimize government spending on inefficient bureaucracy, but I'm very skeptical. What if they can look at my details and my own private information if I start to use digital identification?*



## Cyber security

Large electronic data sets containing immense amounts of personal information are attractive targets for cyber attacks, which is a threat of increasing urgency for governments and private sector organizations globally.

In India's Aadhaar example, the system was marred by shortcomings attributed to problems in project design and inability to adhere to the duty to protect. Lack of such controls led to a 2018 data leak that made Aadhaar data on 200 official government websites public. The problem was so rampant that a simple Google search would reveal thousands of databases along with demographic data including Aadhaar numbers, names, names of parents, Personal Account Numbers (PAN), mobile numbers, religion, marks, the status of rejection of applications, bank account numbers, IFSC codes and other information.





## Cost, complexity and collaboration

### Case study: Australia's Trusted Digital Identity Framework (TDIF)

---

Since 2015, Australia has been pursuing a whole-of-government digital identity program guided by requirements set out in the government's TDIF guidance and requirements. The program aims to provide identity verification across a range of government services and private sector offerings.

Despite significant investment of government funding and resources, legislation to implement this system had not yet been passed as of mid-2022. The program seeks to establish permanent governance arrangements and a regulatory regime.

In the meantime, the Australian financial sector is forging ahead with developments within the current scope of the TDIF. Australia's big four banks are going to cooperate with Australian Payments Plus to develop its digital identity initiative, ConnectID. The banks will act as identity providers in a series of trials. ConnectID, which last year was accredited to operate a digital identity exchange under the TDIF, will provide an identity exchange linking merchants with identity providers.

Throughout 2021-22, the TDIF has approved several digital identity providers, including Mastercard, Australia Post, the Australian tax office and others. This program supports some public needs and concerns related to pandemic management.

The lessons learned from the Australian example? Focusing on public and private sector needs, with the benefits and security of people at the center of the design, is a winning combination. However, progress requires significant and sustained investment.



# Making sense of digital identity technology and terminology

---

## Digital identity evolution

Digital identity has evolved rapidly and continues to evolve as user experience, security, privacy, and consent management take the center stage. What started as a siloed and centralized approach is now moving toward more federated, decentralized and hybrid models.

### **CENTRALIZED:**

A single organization establishing and maintaining its own version of a digital identity store for its users. Identity of the same person is fragmented across many organizations who may all hold differing identity stores for their own purposes.

### **FEDERATED:**

A single institution is in charge of establishing and maintaining identity across several enterprises. This is less fragmented across a given digital ecosystem.

### **DECENTRALIZED:**

This is a self sovereign or distributed model where the user controls their own identity rather than an institution 'holding' it. In this scenario, digital identity is self owned, independent, and portable across many organizations.

## Latest trends

### Self-sovereign and digital identity networks

---

The most recent digital identity paradigm - **decentralized identity** - with its portable 'self-sovereign identity' concepts, is designed to put the control of digital lives firmly in individuals' hands. This is a paradigm shift in the way we see digital identity, providing users a promise of better security and enhanced privacy through control of the digital footprint of a given identity. It catalyzes the potential for a connected ecosystem where enrolling into a single portable digital identity is all it takes for someone to access digital services in a secure and seamless way.

We see more and more national digital identity programs of this nature being launched by countries in all geographies (i.e. Belgium, Norway, India, Japan, Thailand, Turkey), as they embark on the journey of adopting digital identity to citizens' everyday life.



## Secure and frictionless user experience across public and private sector

---

Omnichannel channel end-customer experience with enhanced security has become an integral part of establishing digital trust. For example, the Fast IDentity Online (FIDO) Alliance developed authentication standards based on public key cryptography, which is more secure than passwords and SMS One Time Passcodes.

For instance, users of digital identity credentials would be able to easily and securely pass on information about themselves to a government or business once and from then on be able to confirm when and how this information can be used for different services. With this “tell us once” capability, a person can be freed from having to manage dozens of passwords, never knowing if one of their services has been compromised. The benefits enabled by digital identity credentials have the capacity to make previously time consuming processes for access to public and private sector services easier while being more secure.

Such enhanced standards and approaches mean that capabilities can exist for users to create and verify their identity in the private sector, and then re-use that identity in the public sector. Similarly, users can create an identity using a public service and propagate use across both public and private sector.

## Standardization on the move

---

Interoperability and compatibility are essential to the adoption and realizable value of digital identity programs, and the emergence of new standards is a key enabler. For example, European regulation on electronic identification and trust (eIDAS) has made interoperability of digital identities in electronic exchanges mandatory. The European Commission has recommended a universal ID wallet that can be used across Europe by 2030. Internationally, standards evolution continues, for example:

- The International Civil Aviation Organization is currently working on the Logical Data Structure version 2 (LDS2). This is the next evolution of the ePassport.
- The International Organization for Standards (ISO) Technical Committee 14 SC17 WG10 has started work on verification standards for mobile driving licenses.
- “Travel Pass” is available from the IATA Mobile Identity Working Group.
- Other examples exist such as like “ISO/IEC 18013”, “FIDO2”, “NIST SP 800-63-3”, and “OIDC Bridges”, among others. The acronyms may be somewhat impenetrable, but all of these advancing standards help lay the foundation for interoperable, compatible, even cross-border identity with the aim of security and trustworthiness.



# Policy design recommendations

## 1: Digital identity policy must be people-centered

### “People’s needs and rights are prioritized”

Digital identity related policy needs to be designed above all on a user-centric basis that prioritizes citizens’ needs and rights and puts individuals at the center of the process. A great strength of digital identity is it comprises many different capabilities that can be used alone or in combination to serve a need, which can enable it to be tailored to current and future needs of the people that are being served.

Digital identity capabilities can reverse the current situation in which people must design their behaviour around services, replacing that instead with services designed around the person.

### \* Digital identity must be **INCLUSIVE**

*“Easily available to all who wish to use it”*

It is essential that digital identity be inclusive, equitable, and accessible to all who wish to use it if its full potential is to be realized on an international scale in the years ahead.

Development of digital identity policy must take into account the digital divide. The needs of different audiences must be identified to provide alternatives and long-term support. Access to identity services have often been more difficult for certain groups, including people who face barriers to access and barriers to utilizing the right documentation or the right tools. Policy should guide services to be designed so that all rightful individuals can get access. Barriers can take many forms including economic/financial, educational, social, medical and mental health.



*I’d like to use more digital services, but both my father-in-law and I suffer from health conditions which makes it harder for us to use tech, and we also are on a really tight budget - we can’t afford it if it’s going to cost more.*

**– JONATHAN**



## \* Digital identity adoption must be **VOLUNTARY**

*“It’s not a mandate and alternative tools will continue to be available”*

While legal authoritative identity credentials are required by governments, new policies must enable people to have the ability to opt-in to use emerging digital credentials, while preserving the ability to use alternative credentials.

““

*I’m getting older. I’m not interested in all of this. But, I still need support in my administrative procedures.*

**– CHRISTINE**

## \* Digital identity must be **RESILIENT**

*“Always available whenever and wherever it’s needed”*

Identity services need to be sufficiently resilient and reliable for the access to benefits or resources that they enable. This includes ensuring that the service and the inputs to the service are available when they need to be. The aim should be to avoid single points of failure. Without this, digital society will not function. The policy and architecture of related services, and the way those services are used, will determine the activity and participation levels required to maintain sufficient availability. The architecture of related policy and services will also determine where denial of service may occur. This should include ensuring that a network user cannot be denied access without a legitimate reason.

““

*I’m on the go all over the world for work, and need to stay connected 24/7. I absolutely expect to access what I need when I need it..*

**– CATHERINE**







## \* Digital identity policy must be INTUITIVE FOR BOTH INSTITUTIONS AND PEOPLE

*“Easy to use”*

In practice, identity services should provide familiar, intuitive, simple and informative user experiences so that users can make good choices. They should also support modern industry standards for accessibility for all citizens and be available for all citizens regardless of their financial ability.

For instance, users of digital identity credentials would be able to easily and securely pass on information about themselves to a government or business once, and from then on be able to confirm and control when and how this information can be used for different services. With this “tell us once” capability, a person can be freed from having to manage dozens of passwords, never knowing if one of their services has been compromised.

The benefits enabled by digital identity credentials have the capacity to make previously time consuming processes for accessing public and private sector services easier, while also being more secure.



*I get really impatient with services that waste my time – I was surprised at how clear, simple and easy it was to use this digital identity credential. My questions and concerns about privacy and security were clearly articulated and addressed.*

– DAVID

## \* PRIVACY must be central to digital identity policy

*“The right to be let alone”*

Digital identity capabilities add a new dimension to the principle of privacy: data minimization. It means that no more information than is needed for the service is to be collected from others. **Data minimization helps to preserve a person’s anonymity (if so desired).**

Policy should guide services to ensure that a person is able to use their digital identity credentials without surveillance, tracking, collusion, or traceability. The exception being those cases where traceability is required by law, strictly needed without any other option, in respect of fundamental rights and under the survey of the applicable jurisdictional judicial power.



*I want to make sure that the only the very minimum information about my life is shared when I pay my taxes, or buy wine, or go to the bank. I need to know that there are safeguards to protect my privacy.*

– CHRISTINE



## 2: Digital identity must foster empowerment

---

### “People are empowered to access and use their identity data for their internal use and for the general interest”

Digital identity that empowers companies, customers, clients, and citizens builds confidence in relationships, expands usage and can promote public participation in community, government and political processes.

Policies must be structured to guide the development of services that allow individuals to safely carry out transactions while also allowing people to conceptualize, enumerate and control relationships with other parties, particularly when it comes to the flow of information.

Policy that enables and guides well-designed digital identity services can help citizens and residents everywhere exercise their rights and upgrade their public participation .

On a wider basis successful digital ecosystems, that are constructed around digital identity, can provide valuable data for governments to address socio-economic challenges, increase political participation and allow people to gain access to much-needed goods and services. An example of this is the work carried out by Imagia in Québec that detects and diagnoses cancer through AI systems driven by medical imaging data. Developments of such scale that serve the public interest are only possible through mass processing of good quality and interoperable health data.

### \* Digital identity must be USER-CONTROLLED

*“People decide what to share, with whom and for what purpose”*

In practice, the implementation of digital identity solutions, and guiding policies, must give people the opportunity to decide what to share, with whom, and for what purpose, with the option to withdraw consent at any time.



*I want to make sure that my identity remains MINE whatever I'm doing with it – so I can decide what happens to my information. I can change my mind if I don't want it used any more with the confidence that I have full control.*

**– DAVID**

## \* Digital identity must be based on **INFORMED CONSENT**

*“When someone wants to verify or use a person’s identity data, that person chooses whether or not to agree to that use”*

Digital identity policy guides user access to, and control over, their identity information so they can share when registering for a new service, or when accessing a service they have already. It provides users with visibility and control over the disclosure and storage of identity information, protecting their privacy with the requirement that they decide what information to disclose, whether and when to do so, and to whom. And it supports minimal disclosure techniques. When the information shared is very sensitive, it is possible to strengthen the security of the consent by adding more authentication steps.

This principle requires precautions in the context of digital advertising. It is important that the use of digital identity is always based on informed consent. This means that the user must have sufficient information to make an informed decision about how and when their digital identity is used.

Similarly, governments and private sector organizations can tailor the types of digital credentials that they may require individuals to validate by means of digital identification, typically based on the level of risk of the transactions involved. For instance, various authentication capabilities and methods can be introduced as needed, based on risks, to secure a transaction. The introduction of “as-needed” verification based on the risk profile of the transaction involved reinforces personal control of one’s digital identity.



*I applied for a credit card the other day and verified my identity digitally. I gave my explicit consent for it to be used, and only needed to share the exact pieces of information about my identity that the bank needed for the transaction and no more.*

**- CATHERINE**

## \* Digital identity must allow **DATA PORTABILITY**

*“People can move their identity data around”*

Digital identity policy must give people the empowerment to control their data for storage or transmission. Users should have clear and manageable access to their personal data and should be free to share or transfer it without undue burden.



### 3: Digital identity policy must encourage trust through governance

---

#### “It is clear who can be held to account”

In the establishment of an ecosystem of trustworthy digital identity service governance arrangements are required to determine how services are implemented and what controls are put in place to ensure that people and identity data about them are safe. Ultimately, services and people will need to rely on regulations and legal contracts to gain a level of certainty regarding how people or entities are protected.

#### \* Digital identity must be **TRANSPARENT**

*“Policies and operations are accessible and understandable”*

People gain confidence in services when the functioning and governance of the service is transparent and understandable. People will want to have confidence that sensitive data is protected. In particular, people will need to know that personal data is processed in line with data protection laws, including obtaining explicit consent from the subject to whom that data pertains, when necessary. People will also need to understand, to some level, the processes used to establish, maintain and secure digital identities. This will be of particular interest to relying parties who may make business decisions based on the digital identity information they receive.



*When I started to use my digital identity, it was reassuringly simple to understand what I was signing up for. Sometimes ‘small print’ is so confusing and legal, but this time I felt like I knew the purpose, and understood the safeguards that are in place.*

– JONATHAN

#### \* **ACCOUNTABILITY** for digital identity use must be well defined

*“It is always clear who is responsible for use of your identity data”*

Accountability is concerned with ensuring all parties act responsibly while upholding their obligations. Of course, no system or organization is perfect so when things go wrong, parties that incur a loss may be entitled to recourse.




*I want to know that if I do use digital identity, then if something goes wrong it will be really clear who can be held responsible to get it back and to make sure I’m not damaged..*

– DAVID

#### \* Digital identity policies require **SECURITY**

*“Appropriately cautious controls are in place and evolving to keep identity data safe”*

Digital identity systems must ensure that peoples’ personal information is securely encrypted, shared with chosen service providers only with the individual’s consent and protected by strict security protocols.



Systems should be designed to avoid single points of failure that will be targets for bad actors to collude or hackers to breach.



*I am tech savvy enough to know that cyber security threats are always evolving – I need to be confident that my data not only isn't hackable now, but that the ecosystem is required to keep my identity secure ongoing.*

– CATHERINE

## **\* Digital identity must encourage INTEROPERABILITY**

*“Identity data works in and across services”*

A key to developing a successful ecosystem is interoperability - the identity system's success in exchanging data with other providers, systems, technologies and databases. Governments must work to build policy that promotes interoperability across private and public service providers on a national basis. Beyond that, there is the challenge of ensuring international interoperability of data and technology.



*Can I use my digital identity in different states? Does the same digital identity in my digital wallet work at my bank, and at my car insurance broker, and to collect my benefits.*

– JONATHAN

Industry, national and international standards play an important role for promoting interoperability.

## **\* Digital identity policy must be FUTURE-PROOFED by focusing on desired outcomes**

*“Policy is carefully crafted with a focus on achieving measurable outcomes”*

Consideration should be given to specific choice of policy language that will remain true to the principles and duty of care outlined above as future technology leadership and societal norms change. In practice, choosing words that describe desired outcomes rather than specific tools, methods, or technologies will help. For example, when asking for proof of identity, policy may require the evidence provided to be verifiably “authentic” versus being “original”.

## **\* Digital identity policy must be developed and evolved to STRENGTHEN PUBLIC AND PRIVATE DIALOGUE**

Considering the current context of disinformation and misinformation surrounding the topic of digital identity, and in order to promote its understanding while adjusting policies before and during implementation, it is imperative to take into consideration the feedback received during a period of public consultation. The implementation of digital identity policies should involve an inclusive process representing a wide portrayal of people across socio-economic backgrounds and geographies.

# Conclusion

---

**Experience has shown that achieving success in this transformation requires government and private sector commitment, resources and a carefully-designed digital identity program that incorporates the elements needed to achieve widespread public buy-in. As previously described, a successful design must be user-centric, efficient and non-costly with adequate privacy, security and user-control measures. Meeting these user-friendly, secure criteria is all the more important at a time when many members of the public have concerns about government overreach or the possibility of their data being misused.**

The contributors to this report note that when digital identity policies are crafted to meet criteria for privacy, inclusivity and user-centric support, it can play a major role in addressing the concerns and needs of users, both on a national and international basis. By basing policy design on input from people that is grounded in principle, and ensuring individual and institutional needs and concerns are paramount – on privacy, data use, interoperability and other issues – governments and organizations can successfully build and sustain digital identity services with the wide public acceptance and usage needed to maximize its benefits.





## Appendix

---

### Methodology for the development of this paper

This HTF-DIACC paper was created through a collaboration of international contributors from EY, McCarthy Tetrault and DTMV working alongside a DIACC Special Interest Group of multiple private and public sector representatives and an HTF-chaired Advisory Board comprising international experts in digital identity, communication, policy and the digital economy.

The HTF-chaired Advisory Board and DIACC-chaired Special Interest Group deployed a subject matter expert consultative approach to develop the paper. The HTF-led Advisory Board was composed of invited public and private sector executives from Canada and France, while the DIACC-led Special Interest Group was comprised of DIACC members, partners, and individuals with general public interest who had experience ranging from executive to frontline development of services and related policy.

#### AUTHORS:



#### CONTRIBUTORS:



#### PROJECT LEADS

**Ménehould Michaud  
de Brisis,**  
Human Technology  
Foundation

**Joni Brennan,**  
DIACC

**We would like to thank the following representatives that were consulted as part of an advisory group to inform the paper development:**

**Muriel Barénoud,**  
Director of Civic  
Engagement, La poste

**Colleen Boldon,** Director,  
Digital Lab and Digital ID  
Programs, Government  
of New Brunswick

**Alexandre Bounouh,**  
CEO,  
CEA-List

**Raphaël de Cormis,**  
VP, Innovation and  
Digital Transformation,  
Thales and CEO,  
Thales Digital Factory

**Anne Darche,**  
Corporate Director,  
Client Experience  
and Innovation

**Anne-Marie Hubert,**  
President of HTF  
Canadian board and  
Eastern Canada  
Managing Partner,  
EY Canada

**Franklin Garrigues,**  
Vice President, External  
Ecosystems, TD Bank

**Ibrahim Gedeon**  
CTO, TELUS

**Suzanne Guoin,**  
President, Canada  
Revenue Agency

**Jonathan Kelly,**  
Sous-ministre adjoint à la  
transformation numérique  
gouvernementale,  
Province of Quebec

**Mathieu Desrosiers,**  
VP Digital identity and  
Open banking, Desjardins

**Charles Morgan,** Partner,  
McCarthy Tétrault

**Jen Mossop-Scott,**  
Associate Partner, EY

**Behnaz Saboonchi,**  
Partner, EY-Parthenon

**Amar Sharma,**  
Senior Manager, EY

**Grimaud Valat,**  
Partner, DTMV

**We would like to thank the following organizations that participated in a Special Interest Group to inform the paper:**

CGI

Desjardins

dHub Group

EY

Global Privacy Rights  
(Formerly OpenConsent)

Human Technology  
Foundation

McCarthy Tétrault

Onfido

TELUS

The AML Shop

Scotiabank

---

## DIACC

Created as a result of the federal government's Task Force for the Payments System Review, the Digital ID & Authentication Council of Canada (DIACC) is a non-profit coalition of public and private sector leaders who are committed to developing research and tools to enable secure, robust, and scalable Canadian digital ID solutions and services. With privacy, security, and choice at the forefront of all DIACC initiatives, the DIACC aims to enable all Canadians to participate safely and confidently in the global digital economy.

### About DIACC Special Interest Groups

DIACC Special Interest Groups (SIGs) provide a mechanism through which to engage our stakeholder community in discussions around a specific interest. They provide an opportunity to connect subject matter experts from around the world, and to broaden conversations outside of our DIACC membership.

A DIACC SIG does not create intellectual property, but rather contemplates a specific question to make a recommendation to DIACC regarding the next steps that should be considered for incorporation into the DIACC strategy and roadmap.



## **HTF**

Created in 2012, HTF is a network of several thousand members that operates in Paris, Montreal, Rome, Brussels and Geneva with the intention of placing the human being at the heart of technology development and putting technology back at the centre of social debates. HTF's mission is to coordinate international multidisciplinary research projects and serve as an interface between academia, society, and the economy. For HTF members, technology must be part of the solution for building a society that is more respectful of everyone.

## **EY**

EY exists to build a better working world, helping create long-term value for clients, people and society and build trust in the capital markets.

Enabled by data and technology, diverse EY teams in over 150 countries provide trust through assurance and help clients grow, transform and operate.

Working across assurance, consulting, law, strategy, tax and transactions, EY teams ask better questions to find new answers for the complex issues facing our world today.

EY refers to the global organization, and may refer to one or more, of the member firms of Ernst & Young Global Limited, each of which is a separate legal entity. Ernst & Young Global Limited, a UK company limited by guarantee, does not provide services to clients. Information about how EY collects and uses personal data and a description of the rights individuals have under data protection legislation are available via [ey.com/privacy](https://ey.com/privacy). EY member firms do not practice law where prohibited by local laws. For more information about our organization, please visit [ey.com](https://ey.com).

## **McCarthy Tétrault**

McCarthy Tétrault is a leading Canadian law firm delivering strategic, innovative solutions to clients in Canada and around the world.

With offices in Canada's major commercial centres, New York City, and London, U.K., our lawyers work seamlessly across practice areas and regions. We advise on all aspects of business law, litigation, tax, real estate, labour and employment law. We also work with all levels of government to develop laws and regulations that shape the Canadian market, in the industries driving Canadian and global economies.

Through our focus on delivering innovative client services and solutions, we are leading advancements in the legal profession and driving value for clients through project management, creative staffing solutions, and providing alternative fee arrangements. Our award-winning MT>Divisions, a group of complementary business lines, support clients with scalable, rapid-launch solutions in business, data, technology management and other on-demand resources.

## **DTMV**

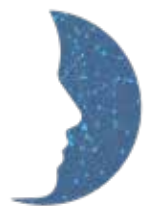
DTMV is a law firm specialized in intellectual property, created in 1984.

Since then, the history, the experience, and the strong relationships between the partners over several generations have created a common vision and passion for the legal profession which enabled a great expansion of both team and fields of expertise, such as digital law.

DTMV's expertise is recognized by the main French and international guides, such as Best Lawyers, Chambers, IP Stars, Juve Patent and Leaders League."



DIACC  CCIAN



HUMAN TECHNOLOGY  
FOUNDATION