SIAPARTNERS

To What Extent Is National Identity Digital?

10 October 2024

Summary

Editorial

The target of our study is to assess the digital maturity of the procedures for citizens to apply for passports, ID-cards or equivalent, across 14 countries. Our results show that the United Arab Emirates (UAE) and Singapore stand out as the most digitally mature countries on these processes. At the opposite end of the spectrum, stand a few countries including Japan, Canada and Belgium. In most countries, the digitalization efforts are not end-to-end and cover only some of the processes. In-person appointments are still a required step in most countries. Within the ID/passport application process, submitting personal data and verifying one's identity is crucial. Very few countries offer a digitalized version of theses steps. Nevertheless, we have observed that most countries have established national digital identity solutions. Despite various formats, we observe a common trend: a disconnection between the physical ID documents (passport, ID card) and the national e-identity used to access online public services. Online Authentication goes through apps and accounts in most of the surveyed countries while ID documents appear only as part of supporting pieces. Singapore and the UAE are ranked at the top of our maturity assessment of the online ID/passport application process and stand out with their prevailing e-identity systems granting access to a wide range of services. It raises the following hypothesis: could their leadership in online applications be linked to their advanced e-identity solutions? Both countries demonstrate specific e-identity solutions where the actual ID documents serve as the gateway for citizens to access various online services. This seamless integration contrasts with the disconnection observed in other countries. The ease of obtaining an ID document and using it to access online services seems a coherent system which could explain the well-developed digitalization of public and private services in the UAE and Singapore. Our study illustrated how other countries appear to search for continuity between e-identity and actual ID documents. It reveals issues it may address, such as interoperability (European Union's 2021 initiative). Official ID documents may offer a common ground unifying online authentication process from one service to another, simplifying the users' journey. We asked ourselves if the next decades would see the disappearance of physical ID cards. Would they become obsolete as the data they carry can be digitalized? Or would a "phygital" model (ID card with a chip) represent an alternative? A continuity between official ID documents and digital identity enhances the mission of governments of ID regulation, surpassing private identity providers. Personal data protection and identity verification to avoid fraud are core issues. Our use cases highlight the importance of legislation to ensure data accuracy. We open our reflection on the fact that maintaining citizens' trust is central. These ambitions cannot be achieved without governments massively investing in digital infrastructures, tackling issues such as sovereign equipment.

What is **national identity?**

Benchmark of online passport/ID application processes and national e-identity devices

A. Introduction

In the 21st century and the widespread adoption of the internet, many governments have embarked on a journey to digitize their engagement with citizens. This transformation is driven by diverse motives including cost-effectiveness, security, inclusivity, and accessibility with the end objective of simplifying the provision of public services at any time and from any place. Furthermore, citizens expect services to be immediate and easily accessible, and digitization provides a pathway to meet these expectations effectively.

Today, the degree of digital maturity not only depends on a country's economic development, but also on other factors such as internet and smartphone penetration, the quality of digital infrastructure and the level of citizen engagement. These differences in digital maturity vary not only by country, but also by industry, depending on the priorities and the investment allocated by each government.

In our study, we chose to focus on identity-related services, meaning the procedures allowing citizens to apply for passports, ID-cards or equivalent. They are central to our ability to access and receive government services, as well as integral to everyday life processes such as applying to educational institutions, participating in legal proceedings, fulfilling tax obligations, and securing employment opportunities.

B. What is Identity ?

Identity corresponds to **a set of attributes associated with a physical person**, enabling that person to be linked to other data. Historically, identity has been proven through face-to-face interactions. In the present day, the emergence of new technologies has expanded the range of options available. Governments at various levels employ diverse methods for individuals to assert and authenticate their identities.

Passports are one of the common means to show and prove identity, regardless of where you are traveling to, or are located. It is accepted by all countries to receive entry, visit and leave, becoming internationally standardized since the

1950s. **In contrast, the ID is not as universally standardized.** Its utilization varies from country to country. For example, in Australia there is both federally regulated ID (National health service, or Federal Government Welfare) and state regulated ID (required when opening bank accounts or collecting parcels at the post office). In Canada, the ID card is regulated provincially and used as a driver's license predominantly. In Europe, citizens are provided with a single identity that can be represented either by a national ID card or a European passport. The documents are used for identity control and are required for accessing essential services.

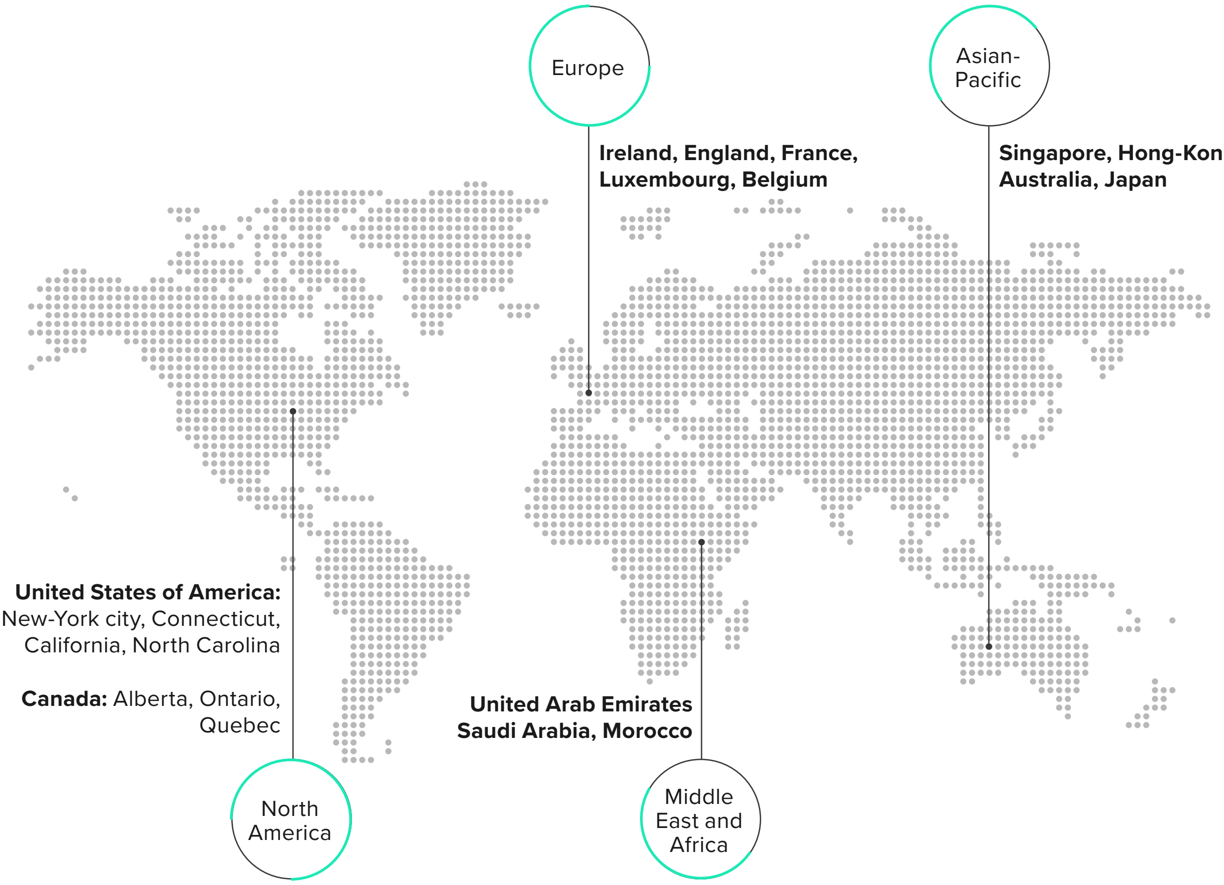
Since ID and Passport documents are central for government services, through the analysis of digital maturity of identity-related application services in 14 countries, we have:

- **Compared the advancement of digitalization of the application process for Passport / ID**, to see only a few countries of our scope achieve a (almost) full digital procedure from the user point of view. We observe in-person meetings remain a norm and question the reasons behind it.
- **Studied the emergence of e-identity devices** and their variety from one country to another. We examine the link between these devices and the actual Passport / ID, as we observe a disconnection in most countries and on the contrary holistic and coherent systems in the top countries of our benchmark. The latter offers a digital way to apply ID documents which, themselves, can be used by citizens to access a wide range of online services.

The study investigates the following questions: What makes the difference between government's advancement into digitalization of their registry processes? Is the ease to apply online for passport / ID not revealing of a broader digital maturity of the country, with ease to access a wide range of online services? Could the close integration of physical and digital ID be the new trend for digitalization? Will the next decades see the end of the "paper" ID card?

C. Methodology of Our Study

Our study is designed to **assess the digital maturity of identity-related services in 14 distinct countries.**


Europe
Ireland, England, France, Luxembourg, Belgium
Asian-Pacific
Singapore, Hong-Kong Australia, Japan
United States of America: New-York city, Connecticut, California, North Carolina
Canada: Alberta, Ontario, Quebec
North America
United Arab Emirates Saudi Arabia, Morocco
Middle East and Africa

To achieve this, we **analyze the process of applying for a passport / ID or equivalent, from a citizen's point of view**, in each country based on a survey encompassing 62 questions. These questions were divided into six categories corresponding to the different **chronological stages in the application process:**

1 → 2 → 3 → 4 → 5

1 Information Discovery

The citizen can:
Find online all the information one needs to prepare its application for passport / ID-card / equivalent

2 Application

The citizen can:
- Formulate the request
- Provide the information and documents needed
- Submit the request to the administration.

3 Payment

The citizen can:
- Choose the modalities and pay the service associated with application for passport / ID-card / equivalent

4 Identity Verification

The identity of the citizen is verified

5 Delivery

The citizen can:
- Receive or retrieve the passport/ ID-card / equivalent one has requested

Additional services:
Assistance throughout the process, Correction procedure, Status tracking, etc.

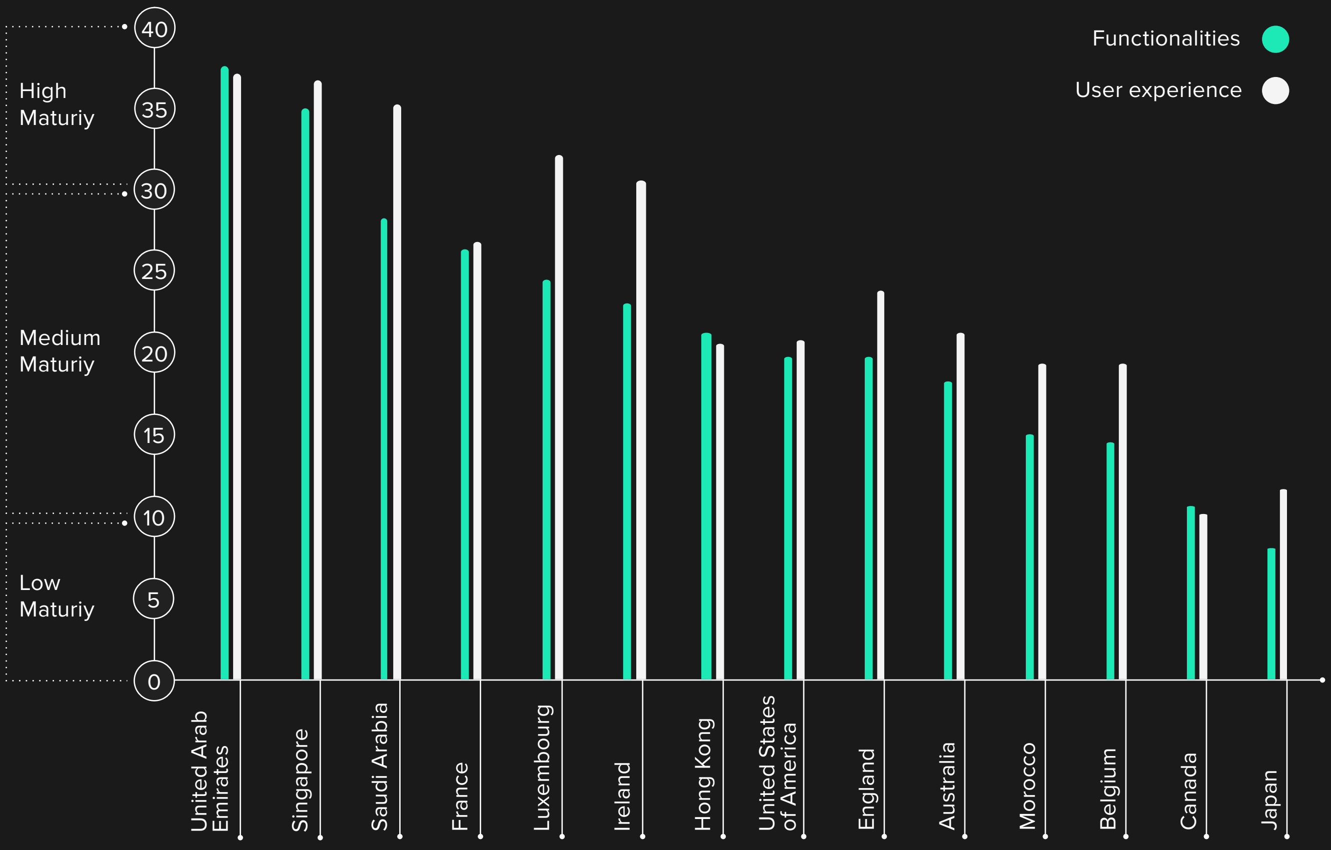
We examined the collected responses through a qualitative framework, aiming to uncover patterns, trends, and discrepancies across the different countries. We evaluate **the digital advancement of each country**, examining the breadth of their online application procedures. We analyzed diverse criteria, **drawing the online services and functionalities** provided by governments on the passport application procedures. We also investigated the potential impact of online or paper-based protocols on the citizen **user's experience.**

These various axes of analysis have been translated into a **grading scale to assess, measure and compare digital maturity of the online passport/ID applications process** from one country to another. Each national online process has been associated with a score regarding online functionality and user experience for the six stages of the service: Information discovery (5 points), application (10), payment (5), identity proving / e-identity (10), passport delivery (5) and additional services (5) (see graphic above).

ID/Passport Applications and E-Identity Devices

Using the methodology and grading scale above, we compared the studied countries with the results below.

Digital maturity of ID/Passport application processes - Comparison of 14 countries



Overall, all the studied countries offer the application for passport and ID-card (or equivalent) online. However, the UAE and Singapore stand out as the most digital mature countries on these processes. Conversely, ID-related services digitalization seems less developed in a few countries such as Japan, Canada and Belgium. Most of the other studied countries obtained a medium score.

To examine these results, we will show that the digital maturity depends on:

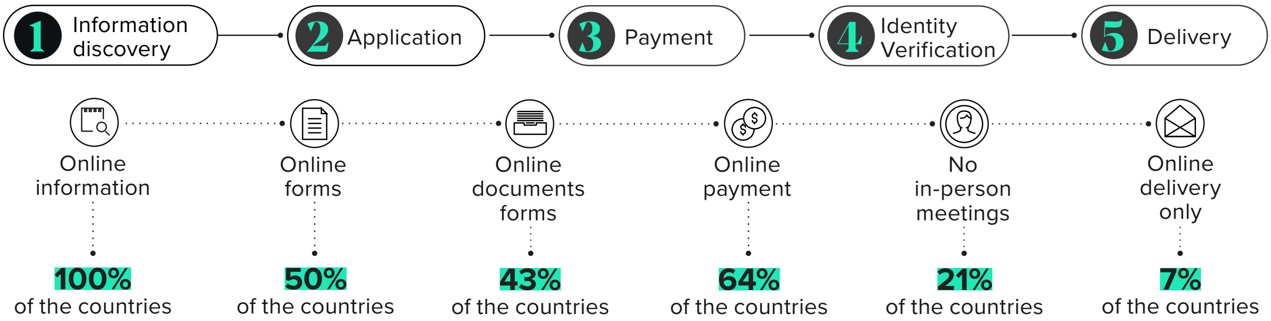
- To what extent can a passport/ID application be completed online, which steps of the procedure are available online?
- To what extent do countries take the opportunities of the digital format to ease the user experience during the process?

A. How Far Can The Application Go Online?

Upon analyzing the data, we classified countries into **three separate categories:**

- **Advanced Digitalization**: This category encompasses countries where the entire application process is either fully digitized or nearly so. Notably, the UAE and Singapore exemplify this advanced stage.
- **Partial Digitalization**: In this group, most of the application process has transitioned into digital realms, yet complete digitalization remains unattained. Countries falling into this category include Hong Kong, Ireland, United Kingdom, France, Luxembourg, and Saudi Arabia.
- **Limited Digitalization**: Here, only a fraction of the application process has been digitalized, indicating a considerable lag in digital adoption. Among the countries represented in this category are Morocco, United States, Australia, Canada, Belgium, and Japan.

Digitalized steps in passport application process - Comparison of 14 countries



1 Information discovery → 2 Application → 3 Payment → 4 Identity Verification → 5 Delivery

Online information: 100% of the countries

Online forms: 50% of the countries

Online documents forms: 43% of the countries

Online payment: 64% of the countries

No in-person meetings: 21% of the countries

Online delivery only: 7% of the countries

Digitalized steps in passport application process - Detailed results

Yes ●

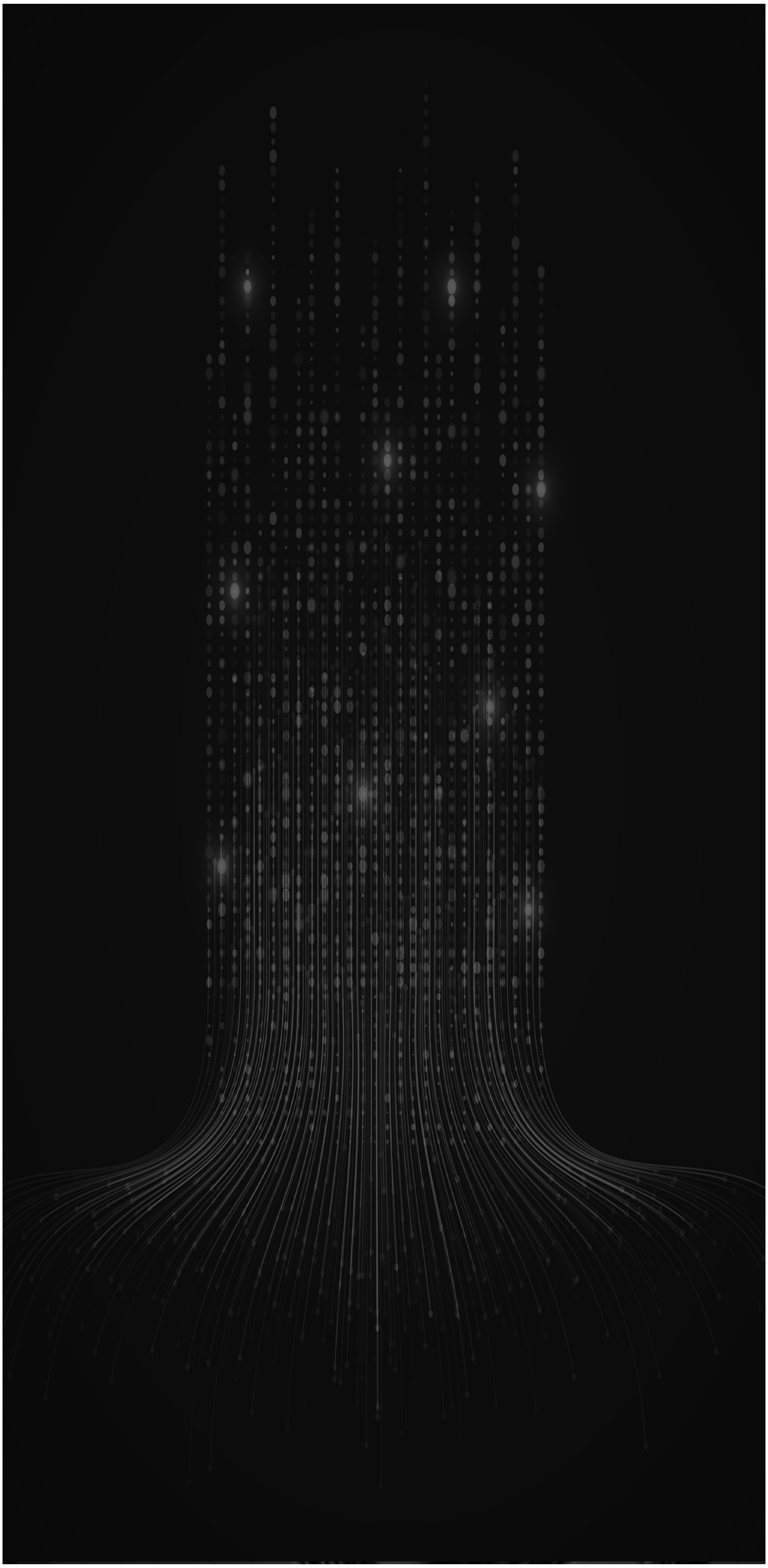
Country	Online information available	Online Form	Submitting Docs	Online Payment	Identity Verification	Online Delivery
United Arab Emirates	●	●	●	●	●	●
Singapore	●	●	●	●	●	*Both physical and digital*
Saudi Arabia	●	●	●	●	●	*Both physical and digital*
Ireland	●	●	●	●		
Hong Kong	●	●	●	●		
United Kingdom	●	●	●	●		
France	●	●		●		
Luxembourg	●			●		
Morocco	●			●		
United States	●					
Australia	●					
Canada	●					
Belgium	●					
Japan	●					
Total	100%	50%	43%	64%	21%	7%

Firstly, while almost no country has a similar application process, **all of them offer comprehensive online resources through dedicated websites for people looking for information.** These resources cover a range of basic passport-related information such as eligibility criteria, application procedures, costs, and the required documentation to apply.

The gaps between countries start to emerge when looking at the possibility for citizens to submit passport applications directly on the website. This divergence highlights a notable gap among the surveyed countries. While half of them provide online application forms, the remaining half either have downloadable forms to print and complete manually or require applicants to obtain them in-person at government offices.

Furthermore, it becomes apparent that the countries facilitating online submission for their citizens tend to extend further digital conveniences by allowing individuals to upload required documentation and conduct payment transactions directly through an online portal. **This inclusive approach streamlines the application process, offering enhanced accessibility and efficiency to applicants.**

Only a few countries such as UAE, Singapore and Saudi Arabia offer a complete, end-to-end digitalized application process. They stand out for their ability to verify identity online and therefore eliminating the need for physical presence. It is made possible through video ID checking appointments (in UAE but also the USA) or through the reliability of e-identity devices (in Singapore). The UAE and Saudi Arabia stand out in the survey as the only countries where in-person meetings are not needed at all, as the government also sends the passport by mail post and provides a digital version of the document.



B. How well are digital features enhancing citizen applications?

Digital maturity may also include a larger variety of auxiliary digital features to accompany the users, helping them navigate easily through their procedures. They represent a further step of digital maturity, taking the best potential of process digitalization.

Our analysis allows for the classification of the passport application process steps into two separate categories:

- **Commonly shared services:** This category encompasses features almost all countries offer to improve the citizen's experience and journey.
- **Developed digital practices and innovative features/functions:** Here, the features implemented are less frequently displayed in the countries of our scope. However, they provide an optimal online experience for the citizen.

Commonly Shared Services

Email assistant
100% of surveyed countries

Saving functionality
75% of surveyed countries

Online booking system
64% of surveyed countries

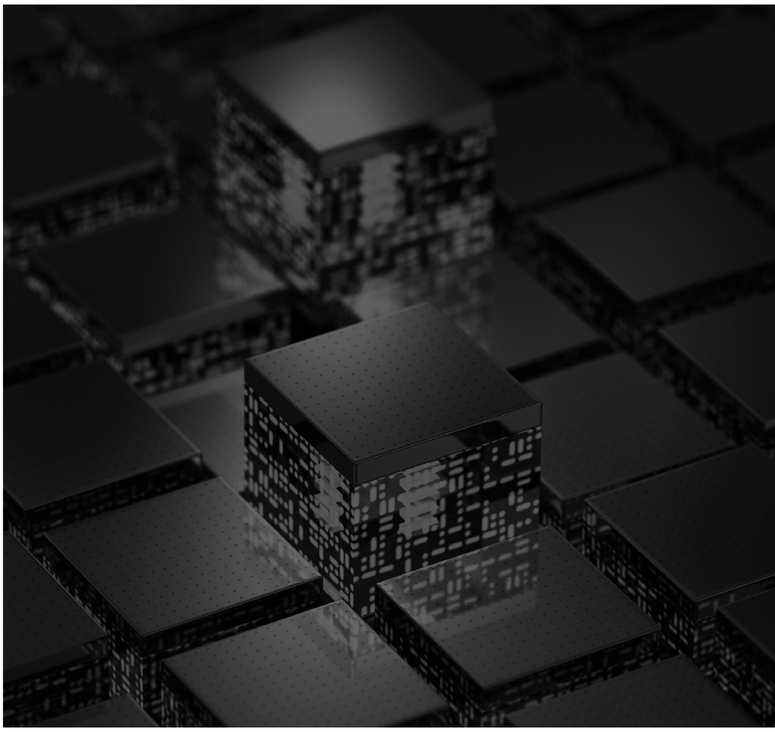
Delivery notification (text or email)
75% of surveyed countries

Status checking functionality
71% of surveyed countries

These functionalities tend to appear as today's standard of comfort offered by online services. They demonstrate the growing interest in reinforcing the citizen's experience. While digitalizing the application process, service owners need to consider the citizens' point of view and needs, for example:

- Reaching out to a representative and ask questions (email assistance)
- Collecting and gathering information or documents from multiple sources and at different times (saving functionality)
- Planning their trips to registry offices, to meet with their commuting and other obligations (booking system and delivery notification)
- Lessening their worry due to uncertainty of the process (delivery notification, status checking functionality)

Therefore, these common functionalities should probably be integrated directly at the beginning of the conception of any digitalized process. **They are "quick wins" for governments starting their digitalization process** and that have not developed them yet.



However, aiming at improving citizens's experience, governments could go further, as some countries in our study demonstrate.

Developed Digital Practices And Innovative Tools

Mobile friendliness
(official application or website with clearly no limitations from a mobile device)
50% of surveyed countries

Autofill payment information
43% of surveyed countries

Chatbot assistance service
Only 3 of surveyed countries, UAE, Singapore, USA

Governments still need to adapt to the prevalence of smartphones in our society. Government should consider a "mobile first" approach as one of the key digital channels for citizen engagement, which will include the application of passports/e-identity devices.

We observed that chatbot assistance is uncommon on the specific scope of Passport/ID application (and public registry procedures), whereas chatbots become more and more present both in private and public spheres. By asking the AI tool, the citizen can directly find all needed information provided by the governments. It represents a way to personalize the user assistance, but with an immediate response time unlike e-mail, phone call, etc.

C. Sia Partners' view

In conclusion of this first section, our survey shows that **the digitalization of the passport/ID application process is still partial in most countries** of the scope. Therefore, the core issue that governments need to **aim at is continuity in the procedure for online users.** It is crucial to **consider the process in its entirety, step by step**: where does the online process "break"? Are there "detours" to physical actions? Is it possible to identify the most important functionalities and online services to implement? The final objective is to improve the fluidity of the application and citizen's online experience. Despite the generalization of digital process, in-person appointments are still required in most countries. The main reasons are:

- **Payment / Document collection / etc. when the service has not been implemented online.**
- **Biometric data collection** (fingerprints, photographs) needed to comply with international standards for passports.
- **Identity verification**, face-to-face is still a prevailing way to ensure that the ID document is applied from and then issued to the correct person.

The two last points are **closely linked to the way governments tackle the issue of digital identity.** We investigate this topic in the following section.

Questioning the role of physical in-person meetings in the passport/ID application process is **crucial when aiming at fluidity** of the procedure. Indeed, **face-to-face visits may lead to "bottlenecks"** as they are conditioned to the number of public officers available. French local administrations experienced such a situation when ID and passport renewal requests accumulate at the end of the COVID19 lockdowns. The first bottleneck in the process for getting the in-person appointment, leading to several months-long wait in some local administrations. This experience may have inspired the French government's recent experimentation of 100% remote process for passport application from the consulate in Montreal. The new process reveals a way of **thinking digitalization step by step. New functionalities have been added to complete the online process:** submitting documents online, video in-person meeting:

Digitalized steps in passport application process France without and with Montreal consulate experimentation

NB : for a remote process (and not necessarily digital), mail post documents delivery is developed in many countries and in Montreal consulate's experiment.

Yes (experimentation) ▨
Yes 🟩

Country	Online information available	Online Form	Submitting Docs
France	🟩	🟩	▨
	Online Payment	Identity Proof	Online Delivery
	🟩	▨	

However, we believe the objective cannot be to totally eradicate physical in-person meetings from the process. The digital divide is a real challenge for administrations, whose services need to be accessible to all. Therefore, developing the online processes should rather aim at **focusing resources on a smaller number of appointments, and improving the quality of accompaniment for citizens who need it the most.**

The second core issue with digitalization is the quality of the **user experience.** This concerns the points of view of the citizen as well as the "internal user", meaning the public officer who deals with the online request. Their perspectives should be central in the design of the digital process. Our survey shows a panel of commonly shared services that are **"quick wins" for governments starting their digitalization process** and have not developed them yet (notification, status, online booking system, etc.).

We have also observed the opportunity to integrate the **latest technological trends**, following the example of the most innovating governments with:

- Ensuring good-quality **portability of the process on mobile devices**
- Taking benefits from **Artificial Intelligence opportunities** such as chatbots but also intelligent documents reading, highly efficient search engines, etc.

Most countries from our survey may also **find inspiration within their own border as these technologies are already well developed in public and private spheres**, but not yet adapted to the passport/ID application procedures.

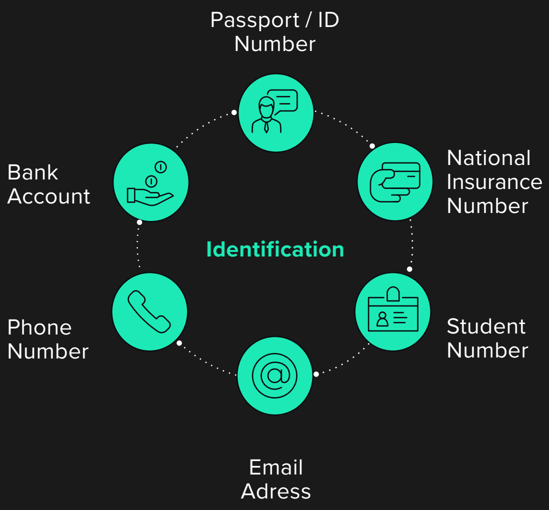
The Link Between **ID/ Passport Applications** and **E-Identity Devices**

Within the ID/passport application protocol, submitting personal data and verifying one's identity is crucial, and is more predominant for ID/passport services than in any other public service. We have seen in the previous section that very few countries offer a digitalized version of this part of the process. However, we have observed that most countries have established digital identity devices. This section attempts to answer the following questions: what is digital identity? What situations does it cover from one country to another? What does it provide? What is the link between ID/passport application process and e-identity devices?

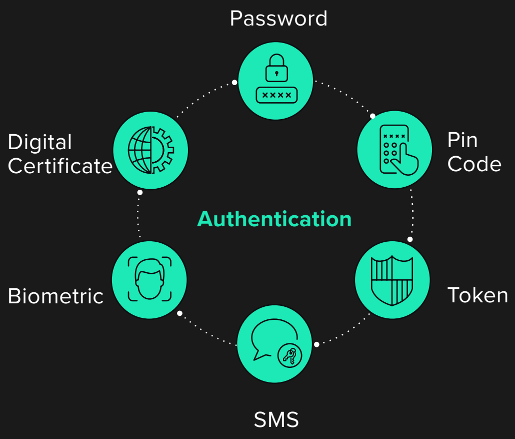
A. What Is Digital Identity Or E-Identity?

Digital identity or E-Identity **is associated with a physical person whose attributes are recorded in digital form and can be used online.** Identity is often used to (1) distinguish one person from another (identify), (2) allow a person to prove that they are indeed themselves (authenticate), and (3) demonstrate identity attributes or characteristics to meet certain requirements (validate).

- **Identification,** which makes it possible **to distinguish one person from another in a given population** (for example through using national identifiers such as national student number)



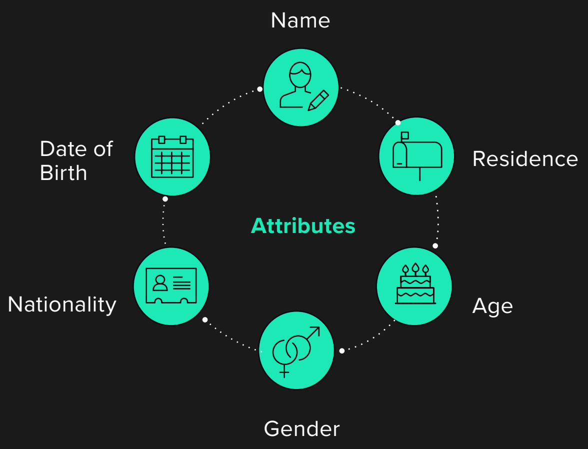
- **Authentication**, which enables a **person to prove that** it is indeed one of his or her identities, for example by providing the password corresponding to an identifier.



Authentication is performed based on the combination of several factors that determine the level of security involved.

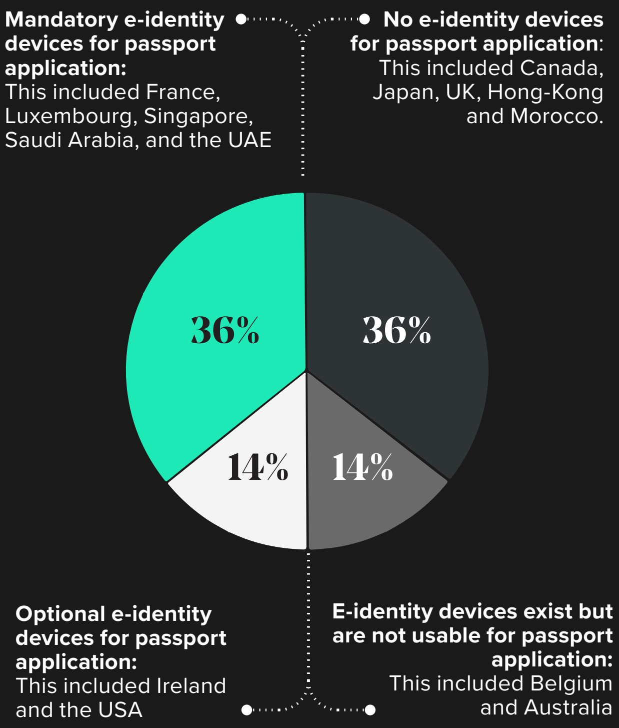
- Who am I ? (Login or identification – e.g. email address)
- Something you are (e.g. Biometric)
- Something you have (e.g. Token)
- Something you know (e.g. Password)

- **Proof of identity attributes**, which makes it possible to **demonstrate identity characteristics** (e.g. nationality, student status, age of majority).



B. What Does Digital E-Identity Look Like Depending On The Countries Studied?

Use of an e-identity device provided by government to apply for a passport comparison of 14 countries



Mandatory e-identity devices for passport application: This included France, Luxembourg, Singapore, Saudi Arabia, and the UAE

No e-identity devices for passport application: This included Canada, Japan, UK, Hong-Kong and Morocco.

Optional e-identity devices for passport application: This included Ireland and the USA

E-identity devices exist but are not usable for passport application: This included Belgium and Australia

Two thirds (64%) of the surveyed countries have developed a form of e-identity. For 36% of them digital identity is a mandatory step when applying for a passport online, indicating an integration of e-identity as an important verification step in the process.

Interestingly, in **21% of the countries, digital identity exists, but it is not used for the online application for a passport.** It may be implemented for other public or private services as in Belgium (bank accounts, postal service, medical prescription, taxes). This could be due to **the history of digitalization in those countries: developed sector by sector/ different government entities, services by services.** It may be undertaken by several administrations or private actors in parallel. For citizens, it will result in more complexity with different ways of authentication depending on the procedures needed.

E-identity devices imply various formats. The most developed trend within the survey scope seems to be the **mobile application.** For example, in Hong-Kong, the App "iAM Smart" is linked to one's ID. When applying online for a driving test, the state website will display a QR code. Flashing it with the app offers the possibility to complete the identification process. A similar device exists in Belgium, Morrocco and the UAE. This model offers two factor authentication. **France demonstrates a particular model: a personal accounts aggregator.** Since 2016, «France Connect" aims at federating various identity providers, both public and private. For example, to identify and access the ID application service, a citizen can, through "France Connect", use their account from tax services or Healthcare number, etc.

Despite various formats, we observe a **common feature:** in most situations, there is **a clear distinction between the e-identity device and the ID documents itself.** It is not the passport, ID-card or equivalent itself that the citizens will use to access online services. Indeed, online Authentication rather goes through Apps and accounts in most of the surveyed countries. On the other hand, ID documents appear only as part of supporting pieces:

- A copy needed to apply for e-identity creation process (situation which can be multiplied when various e-identity devices coexist depending on services/sectors)
- A copy among the documents assembled in the digital identity (being the most commonly shared data with address and photo for the surveyed countries)

Therefore, in most countries, we observe a disconnect between the digital and the physical identity.

Countries also differ on the **prevalence of e-identity devices in citizens' everyday lives.** We looked at which public and private services are accessible through digital identity. In the scope of our study, these are social security (available with e-identity in almost 60% of the 14 countries), closely followed by paying taxes (43% of the countries), and then postal services (29%). Registry services should be added to the list, as we have seen previously that one can use digital ID to apply for a passport in half of the countries (36% systematically, 14% as an option). E-identity is the most prevalent in Singapore and UAE where most public and private online services require identifying using the government digital device.

We choose to take a closer look at their model in the following section.

C. When ID Documents And E-Identity Are Connected In A Integrated System?

Singapore and the UAE are ranked at top of our maturity assessment of the online ID/passport application process, standing out with their generalized e-identity systems that grant access to a wide range of services. It raises the following hypothesis: could their leadership in online ID applications be linked to their advanced e-identity devices? Both countries demonstrate specific e-identity solutions where the actual ID documents, which can be applied for online, serve as the gateway for citizens to access various other online services. This seamless integration contrasts with the disconnection observed in many other countries.

The ease of obtaining an ID document and using it to access other online services seems to be an integrated, whole-of-government approach which could explain the well-developed digitalization of public and private services in the UAE and Singapore.

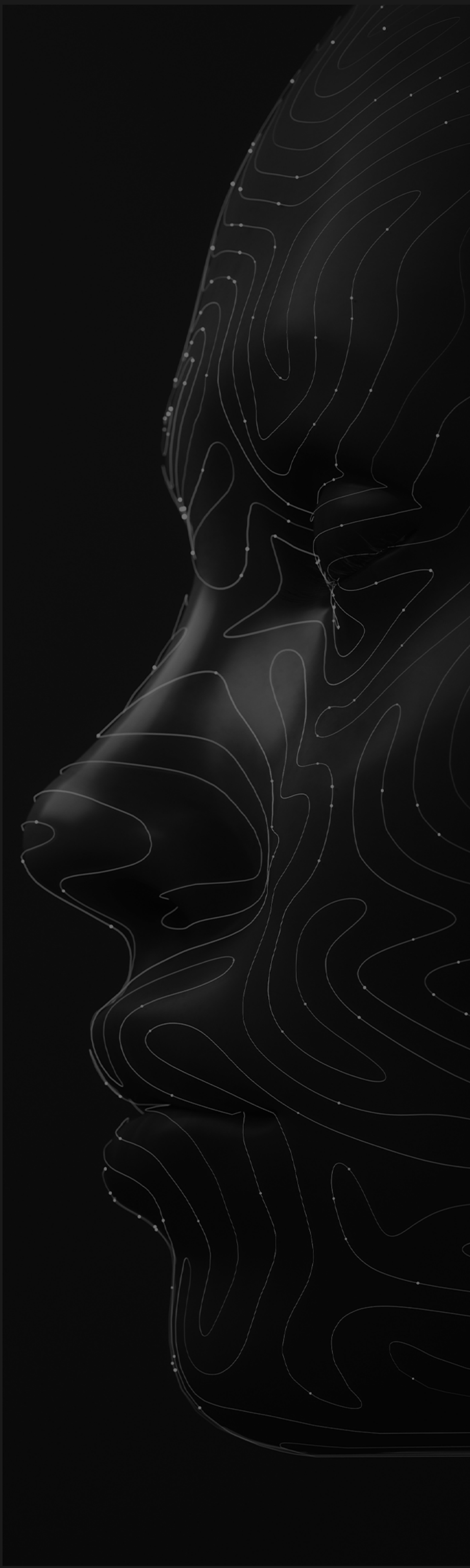
Singapore's and the UAE's integration of e-identity are aspirational and are described further:

In **Singapore**, from birth to death, a person is assigned a NRIC number which is the primary unique identifier for a citizen. The **National Registration Identity Card (NRIC) is integrated with the SingPass digital identity system.** All government services are linked to this number from pension, housing, taxes, marriage, various licensing, and death. This represents more **than 2000 services from more than 700** organizations[1]. In 2022, there were **more than 4.5 million Singpass users**[2]. It also represents 350 million transactions annually[3]. The e-identity is also used by the private sector, but the companies do not have direct access to a citizen's personal details without their consent. This penetration of e-identity in every day's life is possible thanks to the history of its **development since the 1980s.** It was further enhanced through SingPass in 2003,[1]a complete digital identity management platform for authentication, document signing, form filling, and more. It is a fully digital alternative to the physical card.

Legislation was another important lever for Singapore's widespread adoption of e-identity. Singapore's robust legal frameworks such as the National Registration Act and the Registration of Birth & Death Act, allow to provide the **necessary support and trust for citizens and businesses to embrace digital identities.** The ETA establishes the legal foundation for electronic records and signatures, ensuring their validity and enforceability. The Cybersecurity Act was enacted to safeguard critical information infrastructure against cyber threats. This Act ensures that robust cybersecurity measures are in place. It indirectly supports the security of the SingPass system and e-identities by setting high standards for cybersecurity practices. Finally, the PDPA regulates the collection, use, and disclosure of personal data by organizations, ensuring that personal data is protected and managed responsibly. This Act ensures that private sector companies cannot access a citizen's personal details without their explicit consent, thus protecting the privacy of e-identities. **The case of Singapore shows how the legislative framework is a cornerstone when dealing with State digital** identity.

Singapore illustrate this model of "continuity" between ID documents and e-identity devices by combing a strategic vision, robust infrastructure, strong security, legal frameworks, interoperability, and a focus on user experience. This model not only facilitates seamless integration between physical and digital identities but also supports **the broader goal of creating a Smart Nation.**

In the United Arabic Emirates, the approach to digital identity mirrors some aspects of Singapore's model, focusing on continuity and integration between physical ID documents and digital identity systems.



[1] Smart Nation Singapore: Singpass Singapore's National Digital Identity (Factsheet) (smartnation.gov.sg)
[2] Idem
[3] Idem

Since 2018, citizens can use the **Application "UAE Pass"** on their phones. When using it for the first time, users only need to **scan their Emirates ID**, verify their email and phone number using a One Time Password (OTP), and create a PIN. Therefore, the app is directly connected to the Emirates ID which conveys the citizen's email and phone number.

In most administrative procedures, such as passport/ID application, **facial recognition technology** is used to add a level of identity verification, completing the process without needing to visit a government service center. The UAE pass allows access to more than **6000 services**[4]. It includes **all online public services but also the integration of the private sector.** Particularly, the areas of **medical and transactional services** are a significant aspect of the UAE Pass initiative.

For instance, UAE Pass allows users to securely access their health records and medical history across various healthcare providers. This interoperability ensures that medical professionals have accurate and up-to-date information, which is crucial for effective diagnosis and treatment. The UAE Pass can also facilitate the issuance and management of digital prescriptions, which patients can use to purchase medications from pharmacies. In terms of transactional services, for example the UAE Pass can be used to pay electricity and water bills or traffic fines securely.

In the UAE, the legal framework is also robust and constantly evolving, as the following regulation can illustrate: Federal Decree Law No. 45 of 2021 regarding the Protection of Personal Data, Federal Decree Law No. 34 of 2021 on Combatting Rumors and Cybercrimes and the Electronic Transactions and Trust Services Law[5]. The integration of the private sector, particularly in medical and high-tech fields, into the UAE's digital identity system exemplified by UAE Pass, underscores a comprehensive approach to digital transformation. By providing secure, efficient, and interoperable services, UAE Pass enhances the user experience, supports innovation, and strengthens the digital infrastructure of the UAE.

Interestingly, we observe that both in Singapore and UAE, **vending machines are accessible at several government centers, a proven solution to meet with the digital divide**. Indeed, they allow access to online services, using e-identity devices, for citizens lacking computer equipment or needing specific accompaniment.

Our survey shows **other countries who appear to search for continuity between e-identity and actual ID documents**. It reveals issues this connection may tackle, such as interoperability or alternatives ways physical and digital format can be intertwined.

In the **European Union (EU), each member state has developed its own e-identity device**: for instance, app in Belgium, accounts in France or Ireland, a personal identification number assigned at birth in Estonia, etc. **With free movements of EU citizens, digitalization of public services raises a crucial issue of interoperability between national government systems,** starting with e-identity devices. Indeed, in April 2023, a consortium comprising 146 private and public partners, and 19 member states was launched to tackle this problem and test the deployment of a digital identity wallet to simplify and secure online processes for European citizens, focusing on the interoperability of national e-identity solutions through six use cases[6]. For instance, a French citizen finding employment in Germany would see one's relocation simplified if opening local bank accounts was possible with one's French ID.

Looking for a common ground for all countries, the consortium reflections seem to **tend towards continuity between ID documents and e-identity devices**. A solution studied would be to give to official ID documents (national ID card and European passport) a dematerialized version. This new format could be shown from a smartphone and scanned by any public officer (as an alternative to a physical card) but also carry credentials which allow authentication and access to online public services anywhere in UE.

Interoperability objectives also rely on legislation. The electronic identity system in Europe relies on legislation and regulation. The eIDAS (Electronic Identification, Authentication and Trust Services) regulation of the European Union, adopted in 2014, has been a key element in the standardization and mutual recognition of electronic identities across member states. This regulation facilitates the cross-border use of digital services and ensures a high level of security and trust in electronic transactions.

In **Luxembourg**, since 2021, **the physical ID card has included an electronic chip** that contains data such as an image of the ID holder's face, digital fingerprints, national identification number, and authentication and electronic signature certificates as well as related private keys. Similarly to the EU's current reflections, it can be used by citizens with the official governmental application to access online service or be read/scanned directly by a public officer. This e-identity device presents a **"phygital" model** where e-identity and physical card are linked thanks to the chip. It relies on a **technologically advanced infrastructure**, including cryptographical functionalities and stringent security measures on the chip to ensure effective utilization.

However, in our study, **for the "classical" service of ID/passport application, Luxembourg's process is minimally digitalized**. Only payment is possible online, the rest of the process implies an in-person appointment. Indeed, e-identity is more commonly used for private services such as bank or healthcare services. Several Luxembourg banks accept electronic identity cards for account opening, transaction validation, and access to online banking services. Additionally, healthcare professionals can securely access patients' medical records, with patient consent, using the electronic identity card.

[4] Information and services", The Official Portal of the UAE Government

[5] Digital transformation UAE

[6] Electronic Government services, Bank account opening, SIM registration, Mobile Driving Licence, Remote qualified signature, E-prescription

D. Sia Partners' view

Investing in e-identity systems is a strategic move for governments aiming to enhance security, improve efficiency, deliver better services, and foster economic growth. By leveraging technology to streamline identity management, governments can address modern challenges and meet the evolving needs of their citizens.

The benefits of investing in e-identity:

- Improvement of the delivery of public services
- Digital identity as a lever to simplify the process for users/citizens. Within the scope of our study, in most countries, providing e-identity devices (7 out of 10), personal information tends to be pre-filled in the application forms. The user experience is improved, making the process easier and quicker to complete. It may also reduce the risk of mistakes when filling in the information manually. As it stores information provided by governments and sometimes by trusted private sources, e-identity is an opportunity to mutualize these data. Practically, using it reduces the need for citizens to systematically provide the same information and documents for various services in their daily lives.
- Digital identity is a lever to aim at complete digitalization of public services, keeping up with users' demand of accessibility, availability and immediateness. We have seen in our study that, in most countries, the online process to apply for a passport eventually ended with requiring an in-person appointment. The purpose of this last step is for the verification of identity face-to-face, biometric data collection (e.g., fingerprints and photos), and physical document collection. E-identity is one of the ways to offer the possibility of a full distance process, as in Singapore.
- For administrations, it may mean saving costs and time through developing complete digitalization of their processes. Notably, transitioning verification processes from time-consuming manual checks and in-person appointments to a digital and automated way which also increases accuracy and security.
- Fraud prevention: Guaranteeing a person truly is "who they say they are" is essential for governments to ensure the right people get access to the right services and benefits. Furthermore, ID documents provided by governments are among the most forged documents, as they are widely used. Digital identity systems are one way to secure identification, as they allow automation of the verification or two-factor authentication (e.g. with an application).
- Personal data protection: E-identity can be used to give more control to users over the use of their personal data. In some systems, the citizen can choose which aspects of their identity, data and certificates they share with third parties, and keep track of such sharing.

For governments, e-identity is as crucial an issue as national ID card when it is used to provide public services.

We have observed that in most countries **e-identity has been developed as a parallel device to official ID documents provided by governments:**

- On one hand, a physical document citizens need to always carry, mostly used for age and identity control and as "supporting documentation" for any administrative procedure.
- On the other hand, a digital device is usable to identify and access online services. It may carry personal data about its owner but rarely prevents it from providing a copy of physical ID documents or/and an in-person meeting to complete administrative procedures.

Conversely, the different models of Singapore and United Arab Emirates strike us by **the strong connection they show between the official ID documents and digital identity**. We observed in these two use-cases ID documents that are easy to obtain, notably through almost fully digitalized processes, and which themselves give citizens access to large panel of online services.

This reveals a **strategic vision of public services digitalization, aiming at a holistic, end-to-end solution**:

- When governments consider developing online services, the issue of authentication and identity verification arises.
- Governments can state that there already exists a regalian identity, conveyed by official ID documents which can play a more active role than "supporting documentation".
- This logic implies that ID documents are easy to obtain (application process) and can be used as gateway to online daily life services (digital identity device).

This reflection unravels the thread of all questions to be answered to ensure access to digital services in a continuous fluid way for citizens. We see it as a good starting point for seamless online services integration. We believe it to be **a factor of the high maturity and development of Smart Nations as Singapore and UAE.**

In most countries of our survey, e-identity appears as specific formats, disconnected from ID documents. Moreover, they are often plural (Welfare online account, Taxes online credentials, etc.), as digitalization has historically been developed sector by sector, service by service and we have seen that none of the surveyed countries have a digital identity as generalized as in Singapore and UAE. For citizens, it means multiplying "e-identity" application processes, reinforcing the feeling they always have to provide the same "supporting documentation", including ID copy. **Using official ID documents may offer a common ground unifying online authentication process** from one service to another.

Easing the users' journey and experience, it may remove an obstacle for developing online services' use to a massive scale.

The opportunity for "common ground" seems to be exploited by the European Union consortium **to achieve interoperability**. Their reflections may be **interesting material for federal states**, where several state/provincial IDs coexist. Is creating a "new" federal digital identity not adding more complexity? It often constitutes one additional device from the citizens' point of view. To the contrary, the EU consortium chose to use the existing national IDs, in a digital version, as supporting documentation. It focuses discussion on the data and certificates they must carry to ensure interoperability from one national service to another.

Incidentally, **digitalization of ID documents** (passport and ID card or equivalent, driving license, etc.) appears in current reflections. In Singapore, UAE and Saudi Arabia, they are already issued in both formats: physical and digital. We observe that experiments are aligned with the scope of our study. France for instance has introduced digital driving license since 2023, as a first step towards a "digital wallet", compatible with European objectives on e-identity. **In the coming decades, will ID cards and passports disappear in their physical shape?** Would they become obsolete as what they carry can be digitalized, in order to improve the continuity of online users' journey? The trend does not seem confirmed yet. If countries remain attached to physical documents, it may be caused by:

- Habits and the challenge of change management within administrations but also for citizens
- The vast project of internal processes' digitalization for the administrations, looking beyond the citizen/beneficiary's experience (new procedures and equipment needed for public officers to process digital documents)
- The issue of digital divide between citizens

Luxembourg's **"phygital" model** (ID card with a chip used with the government application to access to online services) represent a "**compromise**" for governments and citizens attached to physical formats. Many national ID cards now have chips to carry biometric data, based on international recommendations. However, in our study, Luxembourg does not to correlate with a coherent and broad digital services system. As it is more commonly used for private services, it is not yet developed as a starting point for digitalized public services. Nevertheless, it could be **an alternative model to the "100% digital" model to explore for the next decades.**

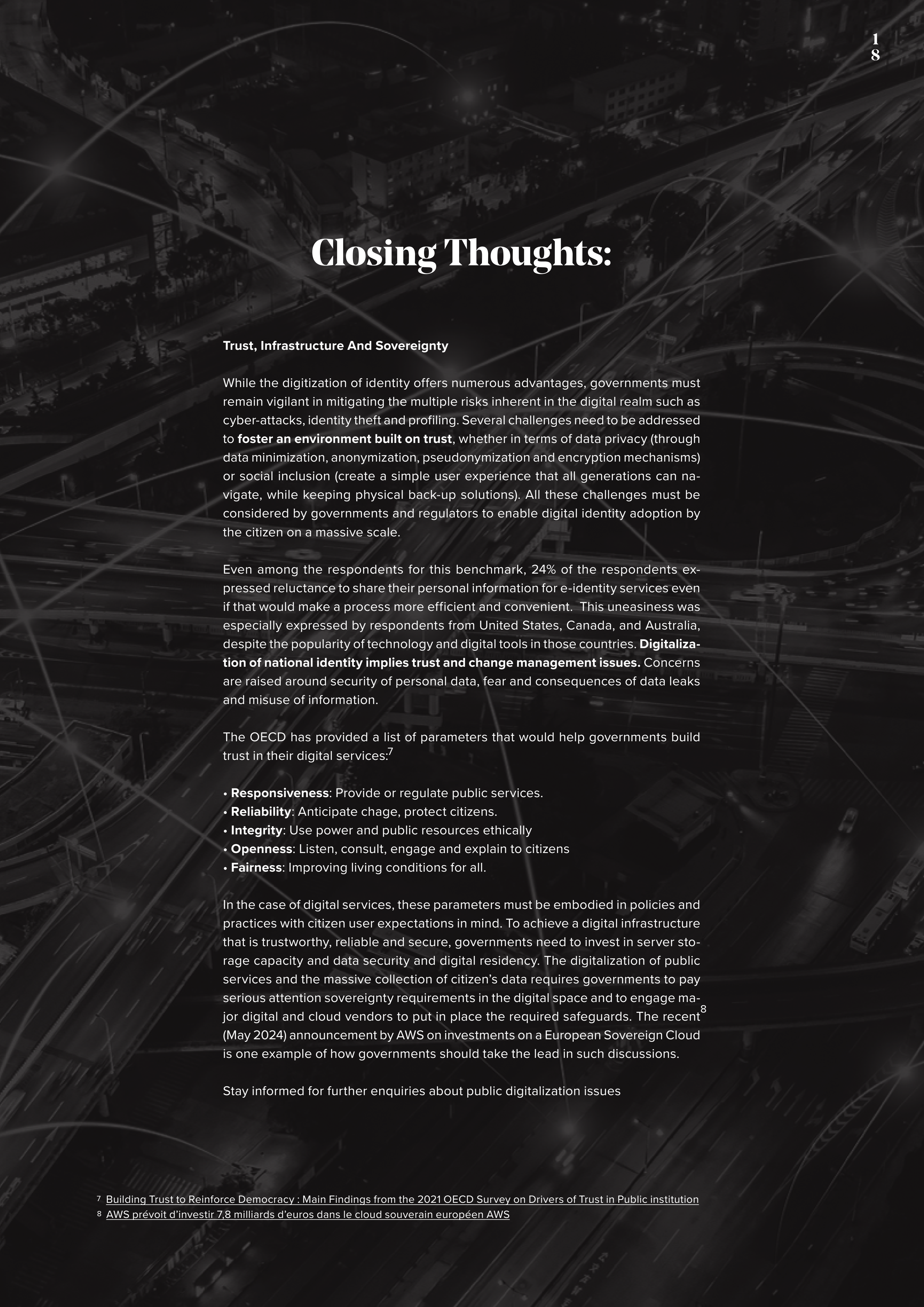
Our study shows the **private sector may provide a critical impulse in services digitalization**, as we have seen in UAE and Luxembourg, with particular roles for the banking and health sectors. Their innovative approaches can be inspirational for governments. Moreover, creating bridges between public and private online services helps to achieve a coherent system from citizens' point of view. Indeed, they both contribute to the basic services for daily needs.

However, **in Singapore and UAE's models, the national mission of governments of ID regulation is enhanced.** Public and private services rely on the official national identity, ID cards. More control may simplify governments' action to protect citizens personal data.

Personal data protection and identity verification to avoid fraud are core issues for governments managing e-identity devices. UAE government makes use of **high-tech** such as facial recognition to enhance the security of the process. But our study of Singapore, UAE and EU's cases especially highlights the **importance of legislation**. The legal frame is crucial to determine **security standards, regulate personal data storage and utilization**. It is also a tool to **systematize the use of governmental e-identity** and integrate it at the core of any administration.

We see that the Singaporean government has gone the furthest on the matter: the National Registration Act and the Registration of Birth & Death Act ensures that the data is always updated, with mandatory use of NRIC number and SingPass, from birth and penalties for not updating personal data (e.g. change of address).

We also believe that national e-identity and public digital services ambitions imply crucial investments in digital infrastructure, which we specify in the following section.



Closing Thoughts:

Trust, Infrastructure And Sovereignty

While the digitization of identity offers numerous advantages, governments must remain vigilant in mitigating the multiple risks inherent in the digital realm such as cyber-attacks, identity theft and profiling. Several challenges need to be addressed to **foster an environment built on trust**, whether in terms of data privacy (through data minimization, anonymization, pseudonymization and encryption mechanisms) or social inclusion (create a simple user experience that all generations can navigate, while keeping physical back-up solutions). All these challenges must be considered by governments and regulators to enable digital identity adoption by the citizen on a massive scale.

Even among the respondents for this benchmark, 24% of the respondents expressed reluctance to share their personal information for e-identity services even if that would make a process more efficient and convenient. This uneasiness was especially expressed by respondents from United States, Canada, and Australia, despite the popularity of technology and digital tools in those countries. **Digitalization of national identity implies trust and change management issues.** Concerns are raised around security of personal data, fear and consequences of data leaks and misuse of information.

The OECD has provided a list of parameters that would help governments build trust in their digital services:[7]

- **Responsiveness**: Provide or regulate public services.
- **Reliability**: Anticipate chage, protect citizens.
- **Integrity**: Use power and public resources ethically
- **Openness**: Listen, consult, engage and explain to citizens
- **Fairness**: Improving living conditions for all.

In the case of digital services, these parameters must be embodied in policies and practices with citizen user expectations in mind. To achieve a digital infrastructure that is trustworthy, reliable and secure, governments need to invest in server storage capacity and data security and digital residency. The digitalization of public services and the massive collection of citizen's data requires governments to pay serious attention sovereignty requirements in the digital space and to engage major digital and cloud vendors to put in place the required safeguards. The recent[8] (May 2024) announcement by AWS on investments on a European Sovereign Cloud is one example of how governments should take the lead in such discussions.

Stay informed for further enquiries about public digitalization issues

[7] Building Trust to Reinforce Democracy : Main Findings from the 2021 OECD Survey on Drivers of Trust in Public institution
[8] AWS prévoit d'investir 7,8 milliards d'euros dans le cloud souverain européen AWS

Your contacts

Bertrand **Lemoigne**

Partner
Government
Paris
bertrand.lemoigne@sia-partners.com

Pierre **Artaud**

Partner
Government
Paris
pierre.artaud@sia-partners.com

SIAPARTNERS

About Sia Partners

Sia Partners is a next-generation management consulting firm. We offer a unique blend of AI and design capabilities, augmenting traditional consulting to deliver superior value to our clients. With expertise in more than 30 sectors and services, we optimize client projects worldwide. Through our Consulting for Good approach, we strive for next-level impact by developing innovative CSR solutions for our clients, making sustainability a lever for profitable transformation.

www.sia-partners.com