The Digital Identity Lobby in the EU and Singapore: A comparative analysis of lobbying strategies in different institutional contexts

Hilten, Stijn van

The Digital Identity Lobby in the EU and Singapore

A comparative analysis of lobbying strategies in different institutional contexts

Stijn van Hilten, s2491559

Thesis Supervisor: prof. Arco Timmermans

Master's thesis in Management van de Publieke Sector: Bestuur & Advisering

Word count: 12487

Date: 18/02/2026

Foreword

This thesis combines my professional work experience on the European wallet-infrastructure with my academic interest in lobby routes and comparative public administration. It aims to showcase how both the chosen technical implementation of a wallet-infrastructure and a different institutional context alter the lobby strategies of corporate actors.

It was difficult to combine both my full-time job and the MSc Management of the Public Sector full-time. I want to thank prof. Arco Timmermans, as without his support, trust and flexibility I would not have been able to complete this programme. I also want to thank my family and my friends for their support, patience and flexibility in rescheduling meet-ups last minute when I had forgotten a deadline for study or was in a crunch.

I hope potential readers of my thesis find the comparative analysis between the lobby surrounding the wallet-infrastructure of the European Union and Singapore interesting and that they will be inspired to look at policy decisions with a comparative lens more often. Without further ado, I hope you enjoy this thesis.

Table of Contents

1. Introduction

More than 5.3 billion people, nearly two-thirds of the world's population, use digital wallets like Apple Pay and Google Pay (Juniper Research, 2025). In countries such as China, the Philippines and Vietnam more than 75% of the population already pays with their smartphone, as well as identify themselves purely through the use of credentials stored within a wallet-app on their smartphone (Juniper Research, 2025). The European Commission has launched the European Digital Identity Regulation (EUDI, also known as eIDAS 2.0), which aims to regulate and safely introduce wallet-apps within the European Union (Regulation 2024/1183). Each member state must provide at least one EU Digital Identity Wallet (EDI-Wallet) to all citizens and residents by the end of 2026, which can be used to identify the user to public and private online services (European Commission, 2025). The EDI-Wallet would allow users to store a driver's license digitally, bank cards, diplomas, flight tickets, and similar personal information securely and conveniently. This European initiative is an attempt to provide a safer alternative to apps such as Apple Pay, which starting from the end of 2025 will also allow US citizens to store their passport or state ID on their iPhone (Apple, 2025). Meanwhile, in Singapore, Singpass launched on the first of March 2003 as a national digital identity platform (Information and Media Development Authority 2018). Over the years, it has evolved, with a major expansion beyond a simple digital identity platform to a wallet, which allowed private sector services, in March 2021 (GovTech, 2021). Currently, 97% of Singaporean citizens aged 15 and above use Singpass to identify themselves for public and private services as well as to pay or transfer money (Ministry of Digital Development and Information, 2022). Due to Singpass' high adoption rate, as well as their working and successful wallet infrastructure, it becomes worthwhile to compare its development and implementation to the EDI-wallet.

Due to the (potential) size of this market, lobbying activities have also been intense. This, in part, may be because the global mobile wallet market is booming, with a size of $10 trillion USD in transactions in 2024 and an estimated size of $17 trillion USD in 2029, a 73% projected increase (Thunes, 2025). The possibility of gaining or losing even a small fraction in transaction fees of this transaction volume means that there is a large financial incentive for corporations to lobby and influence the future's next payment infrastructure. Within Europe this occurs both in Brussels, in the European Parliament and the European Commission, as well as on the national level. An open consultation of the proposed eIDAS 2.0 regulation led to 318 formal contributions and a targeted stakeholder survey by the European Commission led to 106 replies (European Commission, 2020a). The largest manifestation of the digital identity industry is however not through public consultations, but it is visible in Large Scale Pilots (LSPs), formal vehicles that test the wallet infrastructure and help define further implementing acts for the eIDAS 2.0 legislation (European Commission, 2025). One such example is the EU Digital Identity Wallet Consortium (EWC), which consists of both public and private partners such as Google, VISA, Rabobank, Estonia's Ministry of Economic Affairs and Communications and the Netherlands Enterprise Agency (RVO) (EWC, 2023). Konrad Degen and Timm Teubner credited both the federalized and fragmented nature of the European Union, as well as significant influences by private actors, to the intended creation of a federated wallet infrastructure where multiple wallet providers compete with guardrails to increase trust (Degen and Teubner, 2024).

This in stark contrast to Singapore's wallet infrastructure, which is primarily state-owned and controlled. In a study by the World Bank, Singpass' success is accredited to early intergovernmental coordination, ensuring that the target architecture was cocreated by governmental agencies rather than private sector partners (World Bank, 2022). Their implementation was top-down and government led, businesses are allowed access to Singpass 'to improve the customer acquisition and business process', yet did not influence the primary architecture (DiResta, 2025). The institutional design of both the EU and Singapore, together with the technical implementation of the respective wallet architectures, shape what type of lobbying strategies are successful. This thesis aims to explain the differences in lobbying strategies in relation to institutional context and the chosen technological implementation.

1.2 Research Question

The main research question for this thesis is: *"How do the lobbying strategies of the digital identity industry differ between the Europe's eIDAS 2.0 implementation and Singapore's Singpass implementation and how can this be explained by institutional differences?"*

This research question adopts a descriptive comparative approach. Its primary goal is not to measure the effectiveness of the digital identity lobby, but in documenting how private actors within the digital identity industry engage with policy makers across different institutional contexts.

To ensure that the main research question is comprehensively analysed three sub-questions have been formulated, each with focus on different core elements of the main research question. The sub-questions also focus on observable, mediating and explanatory elements. These sub-questions are:

1. **Lobbying strategies (observable element):** which specific types of lobbying strategies are used by the digital identity industry lobby?
2. **Type of implementation (mediating element)**: how does the institutional context and policy history of Singapore and the European reflect within the implementation of eIDAS 2.0 and Singpass?
3. **Institutional context (explanatory element):** How does the institutional context and design of the EU versus Singapore constrain or enable lobbying space and lobbying strategies?

1.3 Scientific relevance

This thesis aims to provide a further understanding as to how the institutional context of governments shape and alter lobbying activities. By comparing the European Union's institutional context and the Singaporean institutional context, it becomes clearer how institutional design impacts policy decisions by governments and alter lobbying strategies. As such, this thesis contributes to the field of Comparative Public Administration, a relatively new field of public administration. The European Union and its lobbying mechanisms have been well studied, but beyond generalizations of lobbying within authoritarian governments little nuanced research has been done regarding lobbying within 'consultative authoritarian' governments such as Singapore (Ortmann, 2012).

By applying different lobbying models across two distinct political systems, this study also aims to give empirical insight into how multinational corporations utilize their technological advantage to create stakeholder salience.

1.4 Societal relevance

Various pro-privacy advocacy groups such as Chaos Computer Club warn of the risks of legislation that enables widespread critical digital infrastructure without proper privacy or security guarantees (Lehmann, 2024). The discussion regarding eIDAS Article 45, which privacy watchdogs warned would enable commercial surveillance, showcases the importance of solid legislation for our digital infrastructure (OpenSSF, 2023). By plotting and analysing lobbying strategies, this thesis provides increased transparency and understanding of the digital identity industry lobby to policymakers, journalists and civil society organisations. The EDI-wallet will define what digital citizenship and a modern payment infrastructure means within Europe for the upcoming decade(s), as such, it is crucial to understand the origins of architectural and technological decisions that have been encoded within the eIDAS 2.0 legislation.

2. Theoretical Framework

The research question needs additional specification on three key components: lobbying strategies, the digital identity industry and the institutional context (Europe's eIDAS 2.0 and Singapore's Singpass).

To ensure a proper analysis of both the European Union's and Singaporean institutional context, it is important to first analyse how the institutional context relates to lobbying and why it is a crucial element to understand the space for corporate actors to lobby and their respective strategies. The receptivity and interactions of governments to lobby activities will be studies across different institutional contexts through the use of comparative public administration, defined as "the study of administrative institutions, process, and behaviour across the organizational, national, and cultural boundaries" (Jreisat, 2011). Distinct administrative and governmental traditions form different institutional context that also have differing ways of filtering, interpreting and operationalizing problems and developments into public policy.

This chapter sets up a theoretical model that categorizes institutional contexts on two axes: the degree of centralisation and the degree of resource dependency. As will be expanded upon in this chapter this theoretical model allows for a finer understanding of how policy outcomes, such as legislation or digital infrastructure, like the EDI-Wallet and Singpass, are shaped through institutional design and lobby activities.

2.1 Comparative Perspectives on Institutional Context and Lobbying

Even though comparative public administration is a rather recent field, research has been done regarding lobbying in different contexts such as in the USA versus the European Union or in authoritarian regimes versus democratic regimes. On a more abstract theoretical level, there are certain key choices and characteristics that determine 'the rules of the game' for corporate lobbying activity.

2.1.1 Veto points and entry points

Seong-Jin Choi proposes a theoretical framework for the effectiveness of corporate lobbying within different institutional contexts (Choi et al., 2015). According to Choi there are two main mechanisms that determine lobby effectiveness: veto points in political institutions, which create constraints to policy change, and entry points in political institutions, which determine the opportunities and entryways for corporate lobbying (Choi et al., 2015, 158). Choi's research focuses on the question of whether political competition, which exists more in pluralist and democratic government, hinders (because there are more veto points) or helps lobbying (because there are more entry points) (Choi et al., 2015, 160). Whether or not political competition helps or hinders lobbying is dependent upon the accountability of politicians, as under conditions of weaker electoral accountability a corporation can more easily sway the policy positions of politicians (Choi et al., 2015, 162). Across different institutional contexts it is therefore important to determine what the veto and entry points are.

2.1.2. Centralisation versus decentralisation

These veto and entry points differ in centralised and decentralised contexts. In the logic of entry points and entry points, decentralized or federal systems offer more entry points because power is shared across multiple levels (national and federal) or across different institutions (Kanol, 2024). In these types of systems, such as the European Union, there is often a large amount of 'venue shopping' as lobbying activities can occur across a variety of institutions, for example on both the level of national governments as well as the European Commission's level (Mahoney, 2008). Due to nature of decentralized governments, there is often a larger amount of veto points as well, as for example the European Parliament can still block a proposal from the European Commission.

In centralized contexts, however, the amount of veto points and entry points is often more limited as there are only certain key players. For example, in Singapore, the hegemonic nature of the People's

Action Party and the highly centralized government severely limit the amount of veto points and entry points. Venue shopping is often not possible in highly centralized contexts, as venues are simply limited. A key part of the theoretical model of this thesis is therefore the degree of centralisation, as this is linked to the veto points and entry points, which determine in part lobbying strategies.

2.1.3 Democratic accountability

Furthermore, Christine Mahoney identifies three aspects of the institutional structure of a political system that are crucial to lobbying: the democratic accountability of policymakers, the rules of the policymaking process and the nature of the media system that conveys policy-relevant messages (Mahoney, 2008, 3; 35). Other factors that determine the outcome of lobbying are the issue level (scope, salience, conflict, focusing event, history and type of an issue) and the interest group level (financial resources, membership resources, advocacy type and organizational structure) (Mahoney, 2008, 35-36). Like Choi, Mahoney also identifies electoral accountability as a key determinant of lobbying methods and success.

Mahoney states that in systems where policymakers are subject to direct elections, the policymaker wants to know whether constituents supports or oppose a certain proposal (Mahoney, 2008, 37). Lobbying firms therefore seek to convince the policymaker that there is public support, tactics like letter-writing campaigns, grassroots mobilization and coalition formation is therefore more likely. However, in political systems where policymakers are not directly elected and lack a re-election motive, this is different. Lobbying arguments are often more technical and tactics will focus on one-to-one transfer of information to bureaucrats and technocrats (Mahoney, 2008, 37). The democratic accountability of politicians and policymakers within different institutional contexts determine not only the transparency of lobbying activities, but also in part the type and form of lobbying activities that are possible.

Even though it is more difficult to study power and politics in less transparent governments, such as non-democratic or authoritarian regimes, some inconclusive research still has been done. Stephen Weymouth has found statistical evidence for a higher perceived policy influence in democracies compared to authoritarian regimes (Kanol, 2024; Weymouth, 2012). Interest groups in democracies also often use inside lobbying strategies, whereas in non-democratic or authoritarian regimes lobby groups primarily use close and informal contact with the government (Kanol, 2024, 89).

2.1.4 Resource Exchange Model

Anne Binderkrantz and Helene Pedersen have also developed a theoretical framework that is suitable for comparative analysis. Their ‘resource exchange model’ explains how lobby groups gain access to policy makers by positing that gatekeepers such as politicians, bureaucrats and journalists exchange political standing for specific resources such as funding or technical expertise provided by lobby groups (Binderkrantz & Pedersen, 2024, 192). Information and technical expertise is a key asset in this exchange, as gatekeepers can value technical expertise such as knowledge regarding wallet-infrastructures to draft feasible regulations, publish newsworthy articles or gain a political advantage (Binderkrantz & Pedersen, 2024, 201). Binderkrantz and Pedersen also make the distinction between outsider, such as public legitimacy and media attention, and insider resources, such as technical expertise, economic data or legal knowledge (Binderkrantz & Pedersen, 2024, 200). The effectiveness of a lobby is dependent upon the ‘match’ or ‘trade’ between resources of gatekeepers and lobby groups. According to David Coen, a significant resource dependency has emerged within the European Union, with officials being dependent upon externally provided expertise, information and reputation (Coen, 2007). Helene Klüver’s research also confirms this dependence, as an important factor affecting lobbying groups is the complexity of the legislative proposals and the related policy issues (Klüver et al., 2015a). The demand for input from interests groups relates to the degree of complexity and the amount of policy competence of institutions/governments, it can be expected that lobbying access and influence increases with the complexity of policy proposals, when this complexity necessitates external expertise (Klüver et al., 2015a, 450).

2.1.5 Theoretical model

These two hypothesis form the basis of the following theoretical model. Summarized, the degree of centralisation affects the amount of veto points and entry points within an institutional context and therefore the lobbying routes and targets. The degree of resource dependency affects the influence and access of lobbying actors, as with a higher degree of dependency a better 'trade' can be made.

	Low Resource Dependency	**High Resource Dependency**
Decentralized (Multi-level/Federal)	State has high capacity across many venues. Out of scope for this research.	**Quadrant: The European Union (eIDAS 2.0)** Numerous entry points & high need for info. Lobbyists can trade technical expertise for influence and access to policy decisions.
Centralized (Unitary/Executive-Led)	**Quadrant: Singapore (Singpass)** Few entry points & high state capacity. Lobbying actors cannot easily change policy goals and instead seek policy alignment.	**Quadrant: Concentrated Capture** Few entry points + High need for info. Out of scope for this research.

2.2 Technical Implementation of the European Union and Singapore

For the purposes of this study, the context of both the eIDAS 2.0 implementation and the Singpass implementation will be studied primarily through the pathways the digital identity industry used to lobby to achieve their desired policy outcome. Firstly, it is important to scope both implementations, both technically as well as temporally. Secondly, it is important to define the characteristics of the relevant institutional contexts that are relevant to the digital identity industry lobby.

Not only is the institutional context important to understand which lobbying strategies are utilized by corporate actors, it is also crucial for understanding the policy decisions and policy history by governments. The goal of a lobbying strategy is, to alter policy, is determined in part on the 'institutional momentum' or the precedent and historical context of policies of governments. It is therefore important to understand the reasoning behind policy decisions such as the eIDAS 2.0 legislation and the Singpass implementation, which must be understood from within their relevant institutional contexts.

2.2.1 eIDAS 2.0 Implementation

The eIDAS 2.0 regulation is formally known as *Regulation (EU) 2024/1183 of the European Parliament and of the Council of 11 April 2024 amending Regulation (EU) No 910/2014 as regards establishing the European Digital Identity Framework*. The temporal scope, for the purposes of this paper, will be from the proposal of this regulation in 2020 to its current implementation, which is still ongoing. eIDAS 1.0, its predecessor, was also targeted by lobby activities and several of these lobby actors have since been lobbying eIDAS 2.0. However, the eIDAS 1.0 lobby offers less of a relevant comparison with Singpass as the focus of eIDAS 1.0 was not establishing a digital identity or wallet-framework.

2.2.2 Singpass Implementation

Singpass is more difficult to define, as the Singpass brand has been used for several iterations of various differing technologies starting from its conception in March 2003. The focus of this paper will

be on the latest iteration of Singpass, which integrated a wallet system into the already existing digital identity framework and enabled the private sector to offer their services through Singpass. This period is roughly from 2021 until now, as Singpass is still continuously developing their wallet-infrastructure. This will also be used as the temporal scope for document analysis.

2.3 Lobbying strategies

On top of understanding the institutional context in which policy decisions are made and lobbying actors operate, it also important to properly dissect lobbying strategies and decision. In this paper lobbying strategies will be defined as the specific strategies and tactics through which industry actors attempt to influence policymakers during policy development or implementation (Hillman & Hitt, 1999). Heike Klüver has a more morally charged definition: “techniques that exploit their access to policymakers and regulators to minimise the impact and costs of new regulatory frameworks, and shape them towards their preferences and perhaps, away from outcomes that best adhere to the public interest” (Klüver et al., 2015). For the purposes of this study, this morally charged definition will not be used as its difficult to determine what exactly is best for the public, as well as the fact that exploitation as a term has a moral assumption contained within, which is difficult to substantiate.

According to Aidan Vining, there are five elements to consider in a political lobbying strategy:

1. the choice of the level and type of inclusiveness of the strategy;
2. the choice of the form(s) of argument to be used in persuading the relevant constituencies;
3. the choice of venue(s) to be addressed;
4. the choice of organizational target(s) that will be engaged;
5. the choice of delivery mode—that is, whether political strategies should be implemented directly by firm managers or outsourced to professional suppliers of these services (Vining 2005).

The elements Vining identifies and describes form a solid basis to analyse a specific lobbying actor or strategy as they are relevant choices to form a specific lobbying strategy. However, Vining does not describe more broadly the specific lobbying mechanisms that can be identified across institutional contexts. Robert Gorwa argues that there are broadly two categories of lobbying strategies: direct, which focuses on the policymaker, and indirect, which focuses on other stakeholders (Gorwa et al., 2024). Within those two categories he identified five main strategies:

General type	Specific strategy	Goals
Direct: targeted at policymakers	Access lobbying	Leverage access to policymakers at various levels to negotiate for/against certain policy positions
	Coalition building	Build legitimacy and authority for firm policy positions; use coalitions to increase access to policymakers
Indirect - targeted at other stakeholders	Mobilisation	Leverage access to consumers and/or complementors to persuade them to engage policymakers on a firm’s behalf
	Public relations	Use mediated channels of communication to reach public or segments of the public to make rhetorical arguments about legitimacy of company and benefits of products
	Funding	Create financial incentives for organisations to advocate similar positions to firms; finance research, events, and

		other public-facing outputs that bolster industry arguments

(Gorwa et al., 2024)

The usage of these strategies can be identified within both the European and the Singaporean context. These five strategies can be identified and from this an estimate can be made regarding the predominant lobby routes used.

Specific strategy	Observable indicators (EU)	Observable indicators (Singapore)
Access lobbying	Consultation submission to the European Commission Recorded meetings in transparency register Public position statements	Industry input Meeting minutes (if disclosed or shared) Public position statements
Coalition building	Co-signed consultation submissions Consortia members (EWC, NOBID) Joint position papers	Partnerships/coalition input at GovTech Singapore Consortia members Joint position papers
Mobilisation	Grassroot campaigns via social media Consumer reports Citizen feedback on the European Large Scale Wallet Pilots	Grassroot campaigns Citizen feedback/input in GovTech Singapore or Singpass consultations
Public relations	Media campaigns Sponsored reports/think tank publications Industry backed events Company press releases	Sponsored content in Singaporean media/news outlets Industry backed events Company press releases
Funding	Disclosures of corporate donations Sponsored events Financial support to allied consortia or academics (in annual reports)	Industry sponsorship of GovTech Singapore initiatives Partnership funding in ministry documents

Another categorization of lobbying is Iskander de Bruycker and Jan Beyers inside and outside lobbying. Inside lobbying aims at directly contacting policymakers, through face-to-face meetings, participations in expert committees and providing technical expertise in exchange for access and influence (Bruycker & Beyers, 2019, 6). Outside lobbying aims at indirectly influencing policymakers by mobilizing a broader audience and influencing public opinion, utilizing press releases, public campaigns, protest events and the like (Bruycker & Beyers, 2019, 7). Neither strategy is inherently more successful, both strategies depend on specific conditions to be most successful. For example, outside lobbying is more successful when a heterogeneous coalition is formed, with both business interests and non-business interests (e.g. corporations lobbying together with NGO's and academia) (Bruycker & Beyers, 2019, 29). Inside lobbying is most effective when policymakers lack technical expertise and are dependent upon external expertise to draft effective and feasible legislation (De Bruycker, 2016, 599; Klüver et al., 2015, 6). Legislation can differ drastically in terms of complexity, 'the degree to which a given policy problem is difficult to analyze, understand or solve' (Klüver, 2011, 487).

2.4 Expected findings/hypothesis

This research will document and analyse the differences in lobby strategies between the European context and the Singaporean context. The main expected finding is that decentralized contexts and

contexts that are dependent upon external resources lobbying actors will have a higher degree of influence and access in the policy making process. In highly centralized contexts with strong policy competences, however, the influence of lobbying actors on the policy making process will be limited.

The theoretical model described in section 2.1 is dependent upon two hypotheses:

1. In decentralized institutional contexts that are dependent upon externally provided expertise, such as the European Union, lobbying actors will have a higher degree of influence and access in the policy making process.
2. In highly centralized institutional contexts, with low dependence on externally provided expertise, such as Singapore, lobbying actors will have limited influence and access to the policy making process.

3. Methodology

3.1 Research Design

The primary goal of this research is not to measure the efficacy of lobbying strategies of the digital identity lobby, but to identify how institutional contexts impact lobbying strategies, both in their process (how lobbying strategies are employed) and goal (what the aim of the lobbying strategy is). A descriptive and comparative approach is used to analyse the two case studies of the institutional context of Singapore and the European Union.

To ensure a comprehensive answer to the main research question, the three sub-question each focus on different aspects of the case studies. The observable element, the mediating element and the explanatory element in these questions aim to answer what lobbying strategies occur in each context, how these lobbying strategies differ due to the institutional context and the type of technological implementation and what the goal is of these lobbying strategies in each context.

3.2 Case Selection and Temporal Scope

Singapore's technical implementation of Singpass and the European Union's technical implementation of eIDAS 2.0 have been chosen due to the high amount of contrast and large differences between the two contexts. Both in their institutional design and in the type of technical implementation chosen there are stark differences that make it easier to compare and analyse the two institutional contexts. Another reason for the selection of these two case studies is the the fact that there are clear differences between the type of technical implementation chosen to create a wallet infrastructure.

The temporal scope for this research will be for eIDAS 2.0 case study from the inititial legislative proposal in 2020 to present day, as lobby is still ongoing and not every Member State has implemented a wallet yet. For the Singpass case study the main temporal scope will be from roughly 2017 to present day, as the main focus of the case study will be Singapore's Smart Nation policy goals launched in 2017 and the lobby surrounding the usage of Singpass after its transformation to a wallet infrastructure.

3.3 Data Collection

EU sources that will be in scope for this research are (not limitative): EU transparency register, the European Commission Consultation platform and its submissions on the eIDAS 2.0 proposal, European Parliament's Committee reports, press releases, industry position papers, meeting minutes and news archives.

Singaporean sources that will be in scope for this research are (not limitative): GovTech Singapore white papers and project documentation, parliamentary records, press releases, industry position papers, meeting minutes and news archives.

3.4 Analytical Framework

The institutional context of the two case studies will be analysed through the theoretical model described earlier. The degree of centralisation and resource dependency will be used as the primary characteristics of comparison of the institutional context. Whereas other characteristics could also be used, such as the cultural context and history of the Singapore and the European Union, for the size and scope of this thesis these two characteristics have been chosen to be included in the main theoretical model. To properly analyse the lobbying strategies chosen by the digital identity industry, Gorwa's and Vining's models of lobbying strategies have been chosen. The theoretical model of institutional context and models on lobbying strategies together form the analytical framework applied throughout this thesis.

3.5 Validity and Reliability

The analytical framework used is based upon existing theory to ensure that the observations made are properly linked to institutional variables and existing characteristics of lobbying strategies. This ensures internal validity, however there are challenges in establishing the external validity and generalisability of this research. As the case studies are context specific, it is difficult to generalise the findings to different policy areas or institutional contexts. Due to size constraints, mainly the payment processing sector has been analysed in this research, limiting potential findings of other actors within the digital identity industry.

There are also challenges in establishing the reliability of sources used, as the Singaporean context is much less democratic and transparent than the European Union's context. The main data used in the Singaporean context are government published documents and press releases, which may not be fully transparent regarding the actual lobby routes used. In contrast, formal consultations are made public within the European Union, even though it also impossible to disregard potential undisclosed lobby and its effects in this context.

3.6 Ethical Considerations

The author's professional involvement in the technical implementation of the eIDAS 2.0 legislation may impact objectivity. To combat the potential impact, this research utilizes a descriptive approach rather than a normative approach.

As GovTech Singapore declined formal interviews, no off the record information of professional contacts has been used throughout this research. This research solely used public documents, with one exemption being an internal and restricted after-action report by the Association of Banks in Singapore. This document is available upon request in order to ensure confidentiality.

4. Case Study 1: The European Union (eIDAS 2.0)

4.1 Digital Identity Industry

For the purposes of this study *digital identity industry* will be defined as the organisations whose business model or interests are affected by digital identity policy outcomes and would materially benefit from influencing the policy or implementation decisions. Excluded from this definition are specifically other (potential) lobby organisations, such as privacy advocates, digital rights NGOs and academic institutions. Whereas these do stand to gain from influencing lobby outcomes, the purposes and scope of this study is limited to organizations that stand to gain materially/financially by influencing the digital identity implementation. The organizations that stand to gain can roughly be divided up into three categories:

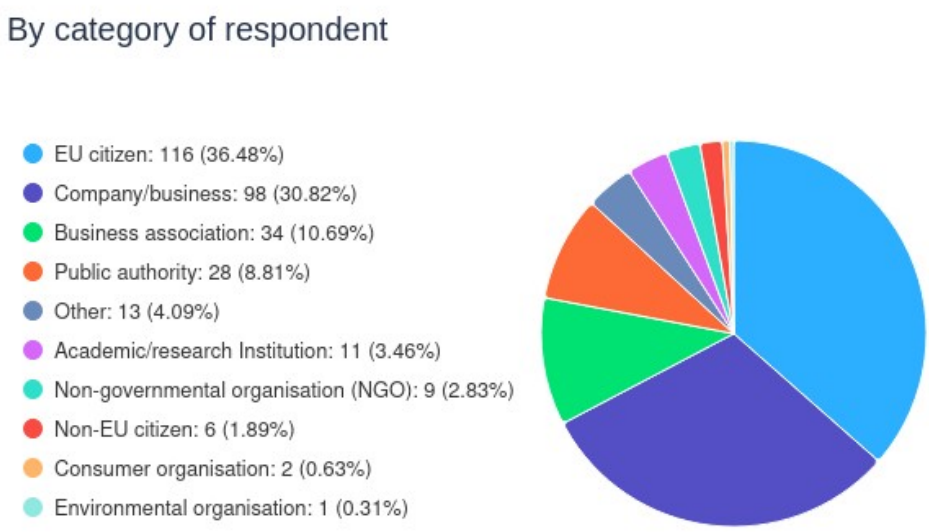
Category	Examples	Reason for inclusion
Online platform providers/tech giants	Apple (Wallet), Google (Wallet), Amazon, Microsoft	Material gain: profit from data access, more users by offering convenient services
Payment processing providers and banks	VISA, Mastercard, SWIFT	Material gain: potential transaction fees
Authentication providers/industry	Thales, Ubiqu, Accenture, Signicat	Material gain: offering of infrastructure and biometric integration, compensation for offering critical infrastructure

(Thoughtworks 2025; iProov, 2020)

4.2 Legislative history

To understand the corporate logic behind the lobby of the digital identity industry in relation to the eIDAS 2.0 regulation several factors must be studied. Firstly, the history behind the legislation and the potential opportunities for corporate actors to lobby the eIDAS 2.0 regulation must be plotted. Secondly, it is important to understand the business model behind of the lobbying actors, as this is the reason why they are lobbying. Thirdly, these opportunities to lobby must be analysed in relation to the European Union's institutional context, as this can explain why specific lobby strategies were employed by the digital identity lobby.

In Ursula von der Leyen's first State of the Union as President of the European Commission in September 2020 she stated that launching a legislative proposal for a secure European e-identity would be one of the European Commission's top priorities (European Commission, 2020b). The consultation for this proposal, one of the largest opportunities to lobby and formally put forward a stance towards the proposed regulation, opened in July of 2020 and closed in October 2020. The consultation resulted in 318 direct contributions and 106 responses in a targeted stakeholder survey (European Commission, 2020a). The make-up of these contributions is as follows:



During the consultation period, the European Commission consulted Member States representatives within the eIDAS Cooperation Network in various workshops and, most notably, held in-depth interviews with 'industry representatives' and 'met business stakeholders in various sectors (e.g. eCommerce, health, financial services, telecom operators, equipment manufacturers etc.) in bilateral meetings' (eIDAS 2.0, explanatory memorandum).

The main goal of the eIDAS 2.0 legislation is to provide, for cross-border use:

- access to highly secure and trustworthy electronic identity solutions,
- that public and private services can rely on trusted and secure digital identity solutions,
- that natural and legal persons are empowered to use digital identity solutions,
- that these solutions are linked to a variety of attributes and allow for the targeted sharing of identity data limited to the needs of the specific service requested,
- acceptance of qualified trust services in the EU and equal conditions for their provision. (eIDAS 2.0, explanatory memorandum)

An ambitious goal, 80% of citizens using a digital ID solution to access key public services in 2030, was also set as a target for this legislation (eIDAS 2.0, explanatory memorandum). eIDAS 2.0 represents a more fundamental shift from governments as mere issuers of physical identity documents to orchestrators of digital infrastructure. One of the main reasons behind the usage of Public-Private Partnerships (PPPs) is because policymakers do not belief governments can deliver the necessary technology and technological innovation (Hoppe & Schmitz, 2021). This reliance on PPPs and external expertise gives private actors the ability to influence decision making and the design of the digital infrastructure to more closely align with commercial interests, effectively forming an inside lobby route due to lack of expertise of the European Commission.

4.3 EU Context: plurality of entry points and veto points

The European Union is widely known for a high degree of complexity and fragmentation, as such there is a high degree of *venue shopping* for lobbyists to find the proper venue to argue their case (Littoz-Monnet, 2014, 1). The European Context, globally, has the following venues for lobbyists:

- The European Commission, the initiator of the eIDAS 2.0 legislation.
- The European Parliament, the legislative body of the EU.
- The European Council of Ministers, a crucial decision-making body containing the Ministers of Member-States

- National parliaments/governments, a target for lobbyists to influence the position of Member States, both within the European Parliament and the Council of Ministers.
- National courts: legal proceedings can form a route of outside lobbying.
- Public opinion: used as an indirect tool to pressure politicians.

The institutions mentioned above each form entry points for potential lobbying actors and can also constitute veto points.

As the eIDAS 2.0 is a highly complex and technical regulation, the European Commission has chosen to further define and establish specifications and standards in various implementing acts, as stated in article 5a: ‘ the Commission shall, by means of implementing acts, establish a list of reference standards and, where necessary, establish specifications and procedures for the requirements referred to in paragraphs 4, 5, 8 and 18 of this Article on the implementation of the European Digital Identity Wallet’. As these implementing acts are also highly technical, the European Commission has chosen to work with LSPs that shape the Architecture and Reference Framework, the Reference Implementation and the implementing acts themselves (Namirial, 2024). The goal of these LSPs are to provide an opportunity to test the reference standards and procedures in a controlled yet realistic environment and to:

- identify any practical challenges or gaps in the implementing acts.
- drive stakeholder engagement, including public sector bodies, private companies, and end-users.
- enable iterative improvements to the implementing acts (European Commission, 2023; Namirial, 2024)

While eIDAS 2.0 was still a legislative proposal and when the European Parliament still needed to vote for the proposal, there was a large amount of outside lobbying to influence positions of Members of the European Parliament. After the European Parliament adopted the eIDAS 2.0 proposal on 29 February 2024, the lobby switched from mainly outside lobbying to a race of participation in the LSPs. These LSPs are:

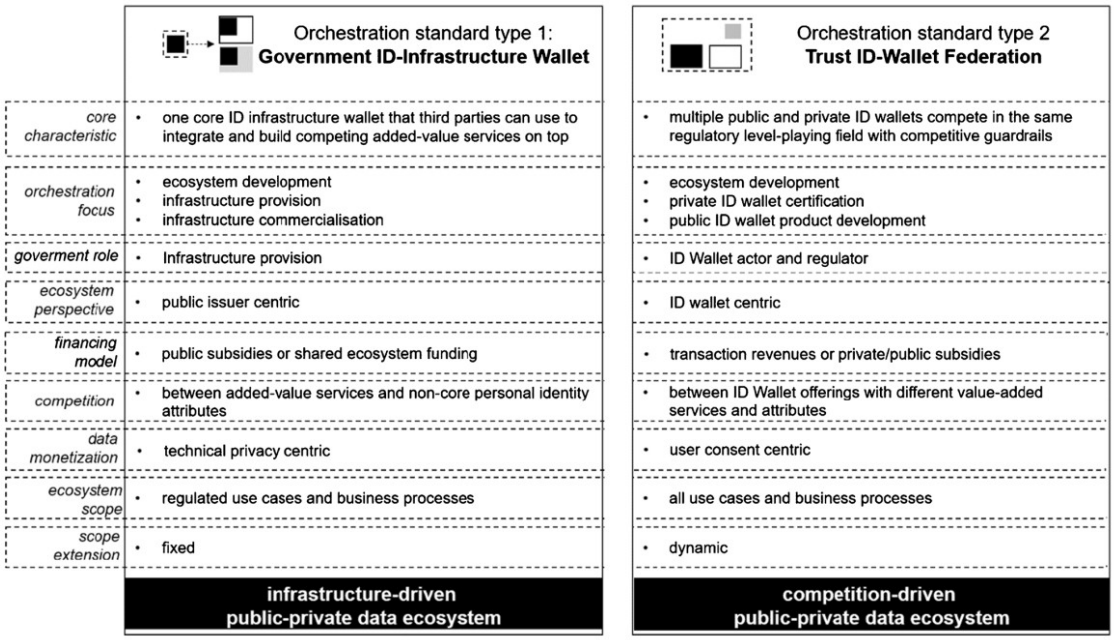
Consortium	**Primary Focus Area**	**Key Stakeholders / Partners**	**Strategic Objective**
POTENTIAL	Government Services (eGov), mDL, Health	19 Member States, Ukraine, IDEMIA, Vodafone. Total of 140 public and private partners.	Functional and technical recommendations regarding the EDI-Wallet implementation; testing prototype wallets; security and privacy analysis. (LSP-POTENTIAL, 2025)
European Wallet Consortium	Digital Travel Credentials (DTC), consumer payments	24 Member States, 80 public and private partners, most notably: Google and VISA.	Leverage travel & payment to drive adoption; test public-private interoperability in high-volume sectors (EUDI Wallet Consortium, 2023).
NOBID Consortium	Payments (Retail, P2P)	6 member states, with private partners, most notably: Amazon, Signicat, Thales, iProov and a collection of Nordic banks.	Integrating the wallet with banks and high-frequency payments; testing SCA compliance and business models (NOBID, 2025).
DC4EU	Education, Social Security	22 member states, Universities, Social	Test complex attribute verification for life events

Consortium	Primary Focus Area	Key Stakeholders / Partners	Strategic Objective
		Security Agencies	(academic credentials/enrolment), facilitating labour mobility (DC4EU, 2025)
APTITUDE	Smart ticketing & check-in, mobility, Vehicle registration certificates	117 public and private partners from 12 European Countries	Demonstrating the interoperability, usability and scalability of EDI-Wallets (Aptitude, 2025).
WE BUILD Consortium	Business and Payment	180+ public and private partners, from 30 countries. Most notably: VISA and Signicat	Streamlining processes for business to business, business to government and business to consumer interactions (WE Build Consortium, 2025).

These LSPs are a prime example of the European Commission's need for outside expertise. The LSPs and implementing acts are formed largely without media coverage and public attention and follow the larger trend of lobbying groups gaining access by providing reliable and quick information that would facilitate credible and implementable policy (Coen et al., 2024, 272). For the purposes of this research, the LSPs that focus on payment will be analyzed, most notable European Wallet Consortium, NOBID Consortium and WE BUILD Consortium. The lobby of the digital identity industry within these LSP's is two-fold: creating a viable business model and protecting existing infrastructure, as adopting completely new infrastructure would be costly.

Business models

Konrad Degen and Timm Teubner's analysis of 'Wallet Wars' explains succinctly the corporate logic driving the digital identity industry's lobby. On the extreme sides of the privatization spectrum there are two views: wallets are public digital infrastructure versus wallets are private tools, of individual citizens, that benefit from a competition-driven approach (Degen & Teubner, 2024, 1). The preference of the digital identity industry is the 'Trust ID Wallet Federation' model, a federated model where multiple private wallets (issued by tech giants or banks, for example) compete for users and trust in a regulated framework (Degen & Teubner, 2024, 17). The following schema covers the key differences in the following models:



One of the most critical areas of lobbying focus is the revenue model for the EDI-wallet, as the eIDAS 2.0 regulations mandates that the usage of wallets must be free for citizens. The industry reply to this is a basic question: who will fund the infrastructure, maintenance and development of the EDI-wallet infrastructure? The most commonly discussed and lobbied industry proposal is the ‘verifier pays issuer’ model, in which the service provider (the service which a citizen uses with a wallet) pays the issuer (the wallet provider) each time a verification occurs (Signicat, 2025). This is the same business model VISA and other payment processors use, taking a fee for each transaction, but would extend to any services used with a wallet, such as authentication for government services. Other business models, such as ‘issuer pays’ or ‘holder pays’, in which the wallet provider itself or the user pays for the transaction costs are seen as less sustainable in a broad public roll-out (Biometric Update, 2025).

In the current eIDAS 2.0 regulation, with some implementing acts already published, Member States will fund the accreditation, supervision and operation of trusted lists of actors that can operate in the infrastructure (Signicat, 2025a). It remains, however, unclear which business model will be chosen by the European Commission, with calls of industry actors to provide legislative clarity as the proposed launch of the EDI-wallet at the end of 2026 is approaching. The lack of clarity has intensified industry lobbying, as profitability of the new EDI-wallet infrastructure is one of, if not, the largest concern for the digital identity industry.

The lobby of the payment industry moved from access lobbying and coalition building to providing technical expertise in the LSPs. One example of an LSP is the WE Build Consortium, an approved pilot by the European Commission with 180+ participating organisations, including 99 beneficiaries and 74 associated partners, covering 27 countries. The consortium started in September of 2025 and includes 20 wallet providers, 13 business register providers, 20 relying parties, 30 Qualified Trust Service Providers (QTSPs), 25 Public Identity (PID) providers, 25 public agencies and has a budget of €25 million (Signicat, 2025b).

The WE Build Consortium is just one of 6 LSPs, across all 6 pilots more than 550 private companies and public authorities are working together to further define the 11 global use cases: digital driving license, authentication, business and consumer payments, consumer banking, educational credentials, health, social security entitlement, telecom, travel, signatures and digital identities for organisations (European Commission 2025c**)**. For the scope of this thesis, the largest digital identity industry lobby focuses on two business cases: business and consumer payments and authentication. Furthermore, the digital identity industry can be split up in 3 key types of corporate actors: payment processing providers, authentication providers and online platform providers.

Payment processing industry

The main focus of the payment processing industry is to transition the use of digital identity from a cost centre, needed for compliance reasons such as Know-Your-Customer obligations or Anti-Money-Laundering, to a potential profit centre. Signicat, a major player in the European digital identity market, published an article titled 'The elephant in the European Digital Identity Wallet room – how can service providers get paid?' in which they argued that only two viable business models exist for EDI-wallet infrastructure: government funding or commercial viability (Signicat, 2025a).

The European Credit Sector Associations (ECSAs) argued in November 2023 that mandatory acceptance of the EDI-wallet in the payment infrastructure of the European Union, specifically regarding the usage of Strong Customer Authentication (SCA) used by the payment processing industry, would lead to a disproportionate cost on the private sector (Rico, 2023). They argued that without a viable business model the mandatory acceptance of EDI-wallet as a payment method would lead to a potential destabilization of the payments processing ecosystem and stifled innovation. In June 2023 the European Savings and Retail Banking Group, a banking sector lobby group, argued similarly and formed a coalition together with the European Association of Co-operative Banks, the European Association of Payment Service Providers for Merchants, the European Banking Federation, EuroCommerce and Independent Retail Europe (Constantin, 2023). In their joint statement they argued that: "If widely used cards and payment processes were included in the new EUDIW Infrastructure on a mandatory basis, huge unplanned investments would be required not only in the financial sector and nearly all merchants in Europe, but also for global acceptance networks. This could possibly result in disproportionate costs for merchants and the payment ecosystem that accept card and account-to-account payments in accordance with the second Payment Services Directive (PSD2) and its successors" (Constantin, 2023).

The threat of disruption of the payment processing industry was used as an attempt to limit the scope of the eIDAS 2.0 legislation but did not lead to an alteration in the final published eIDAS 2.0 legislation. However, the European Commission did decide to further define the scope of eIDAS 2.0 in various technical implementing acts, with a feedback mechanism in the form of LSPs and in the form of formal consultations on the implementing acts (European Commission, 2025).

The WE Build Consortium's lead for the 'wallet for payments' working group is public-private, with the main coordinator being ICTU, an IT-organisation by the Dutch government, with the main technical lead being VISA Europe, one of the largest payment processors (WE Build Consortium, 2025). The focus of this working group is on 4 use cases: consumer banking, consumer payments, corporate banking and corporate payments. The lead for the consumer payments industry is the Dutch Payment Association. The Dutch Payment Association has previously published a paper providing an industry view on eIDAS 2.0, stating that for the payment processing industry it is 'impossible to comply with eIDAS 2.0' mainly due to the usage of SCA (Dutch Payments Association, 2025). To quote them further: "We consider any solutions provided by the LSPs to comply with eIDAS 2.0 to be voluntary for the industry to adopt. A minority of stakeholders participating in LSPs cannot dictate specific implementations for an entire ecosystem" (Dutch Payments Association, 2025). This showcases a fascinating dichotomy: when they published this paper, they were already partaking in the WE Build Consortium to give input to *legally binding* implementing acts (European Council, 2025). This showcases that even as industry is utilizing inside lobby routes, some of the critique outwardly in the form of position papers is still persisting.

5. Case Study 2: Singapore's Singpass

5.1 Introduction

Singaporean Context

Category	Examples	Reason for inclusion
Online platform providers	Grab, Shopee, Carousell, Singlife	Material gain: profit from data access, more users by offering convenient services
Payment processing providers and banks	DBS, OCBC, UOB, NETS, Liquid Group	Material gain: easier customer acquisition and more efficient Know-Your-Customer processes.
Authentication providers	Thales, Assurity Trusted Solutions, iProov, Thoughtworks	Material gain: offering of infrastructure and biometric integration, compensation for offering critical infrastructure

(Thoughtworks 2025; iProov, 2020)

Whereas in the European Union the EDI-wallet is from its conception a public-private partnership, Singapore's Singpass is a top-down and government-led creation. Singpass launched on the first of March 2003 as a national digital identity platform (Information and Media Development Authority 2018). Over the years the technology behind Singpass changed extensively, with only the branding remaining the same. In March 2021 Singpass relaunched itself from a simple tool for citizens to log-in to government services to a digital wallet, akin to the EDI-wallet (Government and Technology Agency of Singapore, 2021). Currently, 97% of Singaporean citizens aged 15 and above use Singpass to identify themselves for public and private services as well as to pay or transfer money (Ministry of Digital Development and Information, 2022). Singpass allows access to over 2700 services, across 800 government agencies and business (Singpass, 2025).

During the initial phase of Singpass, from 2003 to 2017, it was mainly a closed ecosystem fully under state control, with little to no possibility for the digital identity industry to lobby. In May 2017 the Prime Minister's Office (PMO) established the Smart Nation and Digital Government Group (SNDGG), containing:

- "The Smart Nation and Digital Government Office (SNDGO) will beformed under the Prime Minister's Office (PMO) comprising staff from the Digital Government Directorate of the Ministry of Finance (MOF), the Government Technology Policy department in the Ministry ofCommunications and Information (MCI), and the Smart Nation Programme Office (SNPO) in the PMO.
- The Government Technology Agency (GovTech), a statutory board under MCI, will be placed under the PMO as the implementing agency of SNDGO." (PMO, 2017, 1).

The main strategic goals of SNDGG are to 1) apply digital and smart technologies to improve citizen's live, in partnership with other government agencies, industry and the public 2) develop digital enablers and platforms to grow economic value and catalyse innovation by companies and citizens and 3) to drive digital transformation and strength government ICT (PMO, 2017, 2). The SNDGG is the policy and legislative body of the Singaporean digital government, whereas GovTech (formed in late 2016, just before the launch of SNDGG) has become their implementing body responsible for, among others, Singpass (GovTech, 2025).

As the SNDGG had as one of its core goals strengthening cooperation with corporate actors, both SNDGG and GovTech opened up to more input from the digital identity industry.

5.2 Institutional Context

Singapore is a highly centralized and hegemonic one-party state, often categorized as an 'illiberal democracy' as it politics has been dominated by the People's Action Party since 1959 (Lee & Haque, 2006; Ortmann, 2012). Singapore's government can be best described as 'one of executive centrality', where the PMO has strong executive dominance and control over the rest of the government (Aoki, 2015, 214). Bureaucrats are expected to have high levels of productivity, with complete civil service loyalty and discretion (Painter, 2004, 371).

The space for lobby from civil society and potential grass-roots movements is also limited, as in the 1990s the Singaporean government pursued an aggressive strategy of 'strategic liberalization': incorporating and institutionalizing civic society, as they were alarmed at the growing interest of voters in opposition parties when civic issues were not properly addressed (Ortmann, 2012, 16). Public protest and lobby using public opinion is heavily dis-incentivized, as both public protests as well as the media is heavily regulated within Singapore (Chua, 2012, 716). Public assembly and public speeches are licensed to administrative approval under the Public Order Act, with some exceptions for designated indoor talks. As such, there is little real precedent for mobilizing public opinion, both for civic society as well as industry lobby. Outside lobby routes are virtually non-existent in the Singaporean context.

To lobby effectively, the digital identity industry in Singapore had to use inside lobby routes, aligning themselves with the government and policy objectives. One successful example of an inside lobby was from January 2016 when the pilot for MyInfo was launched, a tool within Singpass that allowed citizens to use Singpass to effectively store and save all relevant information to prefill e-services forms (Observatory of Public Sector Innovation, 2024) . While this pilot was running a lobby of Singaporean banks, represented by the Association of Banks in Singapore (ABS) lobbied that they too should be able to use MyInfo, so that citizens could also more effectively use their services and so that they would not need extensive and costly manual Know-Your-Customer processes, as the government would verify the user.[1] This lobby ended up being very successful as in may 2017 GovTech launched a pilot allowing customers to open a bank account with just their Singpass and MyInfo for four banks: United Overseas Bank (UOB), Development Bank of Singapore (DBS), Oversea-Chinese Banking Corporation (OCBC) and Standard Chartered Bank (StanChart) (GovTech, 2017).

In this example, there was a clear indication of coalition building, where the banking sector lobbied through their interest-group ABS, not to change the technical implementation but to gain access to the digital Singpass infrastructure. In their arguments, they aligned with the strategic vision laid out by the SNDGG that citizens would also experience an 80% reduction in transaction time for digital transactions and opening bank accounts. Another argument used was one of economic efficiency, per customer banks saved 50 Singaporean Dollar (roughly 33 Euro) on the elimination of manual Know-Your-Customer and anti-money laundering processes (World Bank, 2022).

The Singaporean context heavily favours lobbying as explicit alignment with policy goals, instead of lobbying to change policy. This can be explicitly seen in the quotes from lobbying banks:

[1] In a restricted after-action report by the ABS, they confirmed that from the beginning of 2016 to September 2018 they were investigating a share Know-Your-Utility tool for all banks to use. They state that 'the project saw unprecedented collaboration between public sector and private sector. AML/KYC expertise, operational expertise and technology expertise was provided to a large degree by the private sector.' whereas the public sector was instrumental in giving access to 'golden sources' of data, such as MyInfo which, together with GovTech, was explicitly mentioned. The document is available upon request.

Mr Jeremy Soo, Head, Consumer Banking Group (Singapore), DBS Bank

"The seamlessness of MyInfo brings us one step closer to our shared vision of a Smart Nation. Customers will enjoy a simpler, easier application process, reducing an estimated 80 per cent of the average time taken to fill in an application. MyInfo will also complement our suite of digital services, where customers are conducting some 60 million transactions via DBS/POSB internet and mobile banking every month."

Mr Ching Wei Hong, Chief Operating Officer, OCBC Bank

"Data is the fuel of the economy, and as Singapore accelerates the creation of a Smart Nation, how data is shared, how easily it flows and how it can be used securely with user consent will determine Singapore's progress and economic performance. The MyInfo platform will enable us to offer customers even more products and services digitally, and leapfrog us into a future of paperless banking." (GovTech, 2017).

In these public statements it can be clearly seen that large banks align themselves with SNDGG and their Smart Nation strategic vision. This led ultimately to it now being common place to use Singpass for financial services. The successful pilot, together with policy goals to further engage industry, led to the transformation of Singpass to a wallet-based infrastructure in March 2021 (GovTech, 2021). In the launch article, it explicitly states that GovTech wants to co-create innovative solutions with the industry:

"Businesses and agencies can tap on Singpass' application programming interfaces (APIs) to enable access or create new value-added services for Singapore residents. The open APIs can be easily integrated with services of organisations, big or small, to enhance customer experiences and improve business efficiency. For example, the use of Singpass for customer logins removes the need for organisations to maintain their own authentication platforms and users can avoid the hassle of managing many different sets of credentials." (GovTech, 2021)

In contrast to eIDAS 2.0, where business models and funding of the digital infrastructure is still being discussed, Singapore's solution is clear: corporations pay to gain access to the Singpass platform (Singpass, 2025). Using Singpass is free for small businesses, whereas larger corporations pay for the authentication volume they use. The core of Singpass and its technical architecture remains, even with the transformation to a wallet-based architecture, firmly under Singaporean governmental control. This is due to Singapore's Ministry of Finance and GovTech forming an architectural committee that ensured ownership of Singpass' target architecture (World Bank, 2022, 9). Singapore explicitly chose a government owned and orchestrated wallet infrastructure, cutting off business cases for the digital identity lobby other than winning government contracts.

Another example of a similar lobby is by SGTech, an interest group of over 1400 Singaporean tech companies such as Accenture, Google, Amazon and Grab (SGTech, 2025a). SGTech also has clear institutional ties, with the chair of the board of governors being Yaacob Ibrahim, who served as a Minister for 16 years (SGTech, 2025b). In November 2022 SGTech published a whitepaper, in which they stated that the Singaporean Digital Trust industry could grow to more than 3 billion Euro (SGTech, 2022). A large part of that projected growth was in digital identity, digital trust consulting and cybersecurity (SGTech, 2022, 20). In the acknowledgments of this whitepaper, the ties between SGTech and the Singaporean Government become more clear, as the Minister for Digital Development and Information is explicitly mentioned as patron of this whitepaper (SGTech, 2022, 36). Unlike position papers and whitepapers within the EU, SGTech's whitepaper does not call for a change in policy, rather it calls for further industry engagement to position Singapore as a world leader in the field of Digital Trust. In doing so, it signals alignment to SNDGG's strategic goals as a field worth investing into to further Singapore's economic growth. As such, it is an implicit and inside lobby.

6. Comparative Analysis

This chapter analyses how the digital identity industry engages with policymakers within two distinct institutional contexts: the European Union and Singapore. By examining the implementation and formation of the eIDAS 2.0 leglislation and Singpass, insight can be gained as to how corporate actors conform and alter their lobbying strategies to different institutional contexts. This chapter also answers each of the sub-questions to the main research question.

6.1 Comparison of Institutional Context

It is necessary to understand that Singapore, although democratic, is also a hegemonic one-party state (Ortmann, 2012). Most literature regarding the Singaporean lobby context is however regarding civil society issues and not regarding corporate lobby activaties. As such, Ortmann's conclusion might be premature when it comes to the digital identity industry lobby. One thing is certain, however, the Singaporean context stands in stark contrast to the European context. The European Union is often defined as multi-level and multi-institutional, which has cultivated its receptive role to lobby efforts quite well (Coen, 2007). Several other differences have been summarized in the following table:

Feature	Singapore	European Union
Political system	Highly centralized, hierarchical, technocratic, with a high degree of policy competence. Often defined as a non-liberal democracy (Guo & Zhang, 2014).	Multi-level, multi-institutional, characterized by a high degree of pluralism (Coen, 2007, 337).
Role of the state/European Commission	The Singaporean state is centralized, a controlling and dominant actor which engages in 'strategic liberalisation', managing change through government mandated constraints (Ortmann, 2012).	Network orchestrator and regulator (Degen and Teubner, 2024). Several venues and entryways to the European commission, ability to go 'venue shopping' (Bruycker and Beyers, 2019).
Primary lobby strategy according to literature	Agenda setting, influencing the national legislative agenda through direct and indirect means (Ortmann, 2012, 21).	With regards to the European Union, one single primary lobby strategy cannot be identified due to the number of venues one can potentially lobby. Most research agrees on a combination of inside and outside lobbying as having the highest chance of succeeding (Bruycker and Beyers, 2019).

6.2 Comparison of Lobbying strategies

This section aims to give a clear overview of the various lobbying strategies used by the digital identity industry in the case of eIDAS 2.0 and Singpass. The main reason for the digital identity industry in Europe to lobby is to ensure that a viable business model can be made and that the industry is deeply embedded within the target architecture (Signicat, 2025a). In Singapore, as the state has full ownership of the Singpass architecture and the lobby was primarily aimed at gaining access to Singpass (World Bank, 2022; ABS Report 2018).

Within the European Union's context there were two stages in the lobbying strategies of the digital identity industry: before and after the ratification of the eIDAS 2.0 legislation within the European

Parliament. Before the ratification the lobby was primarily aimed at members of the European Parliament and influencing the positions Member States within the European Council of Ministers, specificially with regards to the usage of SCA (Rico, 2023). The corporate logic behind lobbying changed from primarily outside lobbying to inside lobbying after the ratification of the legislation, in order to influence technical standards and the target architecture defined in implementing acts.

Within Singapore, the corporate logic of the digital identity industry remained constant: alignment with policy goals. Using Vining's model of decision nodes, the differences in corporate logic can be plotted as follows:

Decision Node	**European Union (eIDAS 2.0)**	**Singapore (Singpass)**
1. Inclusiveness	Before formal adoption of eIDAS 2.0: **Medium**: Industry primarily lobbied with their own respective interest groups, such as the payment industry lobbying through ECSA. After formal adoption of eIDAS 2.0: **High / heterogenous coalitions** Industry actors form broad, transnational consortia, with academia, tech giants (Google, Amazon), banks, and state agencies to pool resources and legitimacy.	**Medium** Strategies are exclusive to partners that already preferred government partners or specific trade associations like ABS or SGTech, that already have existing state legitimacy.
2. Argument Form	Before formal adoption of eIDAS 2.0: **Normative & Technical** Arguments focus on mainly on privacy and reliability of infrastructure. In the case of SCA banks threatened that mandatory accceptance of the EDI-wallet would impact the reliability of existing bank infrastructure. After formal adoption of eIDAS 2.0: **Technical** Industry argued that for the formation of the implementing act highly specific technical knowledge was needed, which the industry could supply in the LSPs.	**Strategic Alignment & Economic Gain** Arguments focus on Smart Nation goals and economic benefits, such as improved efficiency for citizens and banks when using MyInfo.
3. Venues	Before formal adoption of eIDAS 2.0: **Multi-Level (Venue Shopping)** Lobbying targets Brussels (Commission/Parliament) and National Capitals simultaneously. If blocked at the EU level, firms pivot to	**Single-Level (Centralized)** Lobbying is concentrated on the Smart Nation and Digital Government Group (SNDGG) and GovTech.

Decision Node	European Union (eIDAS 2.0)	Singapore (Singpass)
	national implementation pilots. After formal adoption of eIDAS 2.0: Lobbying occured primarily within LSPs, such as the EWC, We BUILD Consortium and NOBID Consortium.	
4. Organizational Targets	Before formal adoption of eIDAS 2.0: **Legislators & Technical Bodies** European Commission, European Parliament committees, and technical expert groups defining the target architecture. After formal adoption of eIDAS 2.0: Primarily other partners within the LSPs.	**Implementing Agencies** GovTech for access to Singpass, SNDGG for further governmental approval.
5. Delivery Mode	**Public & Formal** Executed through public consultation submissions, position papers, open letters, and participation in EU-funded LSPs.	Too difficult to determine due to Singapore’s lack of transparency.

When comparing the various degrees in which Gorwa's five types of lobbying strategies exist in either context, the differences become more clear:

Strategy Type	European Union (eIDAS 2.0)	Singapore (Singpass)
1. Access Lobbying	**High Intensity** Consultation inputs (318 submissions). Tech giants and banks leverage technical expertise to gain access to Commission expert groups drafting the implementing acts.	**High Intensity (Privileged)** Selected access for key players with instutitonal ties and alignment to state goals. SGtech is the go-to and preferred partner for the Singaporean state to interface with the tech industry as a whole and the digital identity industry.
2. Coalition Building	**Formal Consortia** Competitors ally in formal vehicles (EWC, WE BUILD, NOBID) to define standards. These coalitions are heterogenous coalitions improving legitimacy and stakeholder salience. These coalition are primarily aimed at creating or modifying policy.	**Strategic Partnerships** Coalitions are functional rather than political. Example: The banking sector (DBS, UOB, OCBC) uniting to integrate *MyInfo* for KYC and customer acquisition. Coalitions are not aimed at altering policy but at gaining access to state digital infrastructure.
3. Mobilisation	**Defensive Mobilisation** Privacy organisations and web browsers lobbied for key components of the eIDAS 2.0 legislation (Lehmann, 2024). The digital identity industry lobbied very little, as they did not have consumer causes or talking points, but mainly industry concerns, such as the cost mandatory acceptance of wallets for payments. Banks mobilized via the European Credit Sector Associations (ECSAs) to warn of "disproportionate costs" and fraud risks regarding mandatory wallet acceptance for payments.	**Non-Existent** Due to the political culture and regulations on public assembly/speech and lobbying through the media, consumer and citizen mobilisation is not utilized by the industry.
4. Public Relations	**Conflict-Driven** PR campaigns focus on business model viability. Used to create urgency around the lack of a revenue model and the risks of mandatory acceptance of wallets for payments.	**Alignment-Driven** PR focuses aligning the industry as a partner in Singapore's economic growth, complementing policy goals such as SNDGG's Smart Nation.
5. Funding	**EU Grants & Sponsorship** LSP's receive EU funding to run pilots (e.g., NOBID), in which corporations are partners. As such, the digital identity industry actively receives EU funding to further specify the EDI-wallet digital infrastructure.	**Private Sector Funding** The private sector in Singapore receive little to no funding from the Singaporean governemnt, in contrast, they pay to access digital infrastructure such as Singpass.

6.3 Comparison of Technical Implementation

The type of technical implementation and the technical architecture of the EDI-wallet and Singpass vary extensively. Degen and Teubner analysed the two main scenario's of either having agovernment-owned infrastructure or having a federated model (Degen & Teubner, 2024).

As can be seen in the case of the eIDAS 2.0, the European Commission has chosen for a federated model, both to ensure that Member States that can create their own wallets that are interoperable with existing infrastructure and a European-wide Wallet infrastructure, as well as to ensure access, competition and innovation for private actors (eIDAS 2.0 preamble). Because Singapore is highly centralized and because Singapore did not need to interface with a high degree of pluriformity, Singapore chose for a state-owned and operated target architecture, in which all the core functionalities of Singpass were under state control (World Bank, 2022). For the digital identity industry, this meant that instead of lobbying for architecture that could service business interests, the lobby was primarily aimed at utilizing state infrastructure.

The eIDAS 2.0 legislation is not yet implemented and the lobby around the final implementing acts detailing the target architecture is still ongoing (European Commission, 2025). At the end of 2027, all Member States must have launched a public wallet and have the necessary compliance processes and framework ready for private wallets to enter under the eIDAS 2.0 legislation. Because the final design of the EDI-wallet infrastructure is not yet fleshed out but the primary decision for a federated architecture has already been taken, the digital identity industry currently primarily aims at utilizing the LSPs, in which the European Commission outsourced their policy expertise, to act as a co-legislator. Due to the ratification of the eIDAS 2.0 legislation in the European Parliament, the deep core belief of these LSPs has already been set. However, within these LSPs there is still an ongoing debate and lobby regarding the definitive technical implementation. Due to the heterogeneity of the coalition, there is still no clear consensus as to what the specific business models should be and what the technical details of the implementation will be.

The same exists in the Singaporean context, advocacy coalitions such SGTech and ABS cannot alter the main technical implementation of a state-owned wallet infrastructure. However, there is also consensus regarding the usage of existing infrasturcture, as the primary goal of the lobby in Singapore is gaining access to state infrastructure for economic benefits.

Context	**European Union (eIDAS 2.0):** **LSPs**	**Singapore (Singpass):** SGTech and ABS
Technical implementation chosen	The main technical implementation of eIDAS 2.0 is that the EDI-wallet infrastructure will be federated. Participants within the LSPs cannot lobby for alteration.	The main technical implementation of Singpass is that the main infrastructure is state owned and controlled. Advocacy coalitions cannot lobby for alterations due to the Singaporean governmental culture and policy of controlling key infrastructure.
Lobby goals	Within the LSPs there is still an ongoing debate as to what the business model and implementation of wallet	The primary goal of advocacy coalitions is accessing and utilizing wallet-infrastructure for economic

	architecture will be.	benefits.
Lobby origin	The LSPs are specifically funded to generate the secondary aspects of eIDAS 2.0 and must form consensus with all of the participants regarding the details of the eIDAS 2.0 implementation.	Due to the homogeneity of the Singaporean coalitions there is a high degree regarding the goal, maximalization of economic benefits, as such consensus regarding the utilization of Singpass is easier to find.

Within the European context the main goal of actors within the digital identity industry is therefore to gain enough legitimacy to participate in a LSP, thereby gaining formal recognition to act as a co-legislator for the implementing acts. Due to the federated implementation chosen by the European Commission and the lack of technical expertise to precisely mandate how the wallet infrastructure will function within the EU, the digital identity industry primarily uses inside routes to provide technical expertise and ensure the implementing acts will leave room or enable profitable business case. There is a degree of access lobbying to ensure participation within the LSPs, but once entered, the main focus of the digital identity industry is utilizing the legitimacy of the LSPs to alter the implementing acts to be more aligned with business interests. In order to do so the main focus within the LSPs is coalition building to ensure consensus and common input for the implementing acts.

Within the Singaporean context the goal of the digital identity industry is not to act as a co-legislator, nor is it to provide expertise as GovTech and state institutions have a high degree of knowledge or expertise or insource external expertise. Rather, it is to gain access to the existing wallet infrastructure and the economic benefits this entails. As the main infrastructure is state-controlled, advocacy coalitions attempt to signal alignment with state to ensure access. The lobby routes used are inside routes as well, it is much more focused at access lobbying and public relations to signal alignment.

5.3 Comparison of Resource Dependency

The main difference between the European Union and Singapore with regards to the digital identity industry is two-fold: the European Union is more reliant on external expertise and is more fragmented, whereas Singapore is both centralized enough and has enough expertise to provide for their own wallet infrastructure.

This lack of expertise increase stakeholder salience of the digital identity industry in the European Union, by increasing power and legitimacy through LSPs. In the Singaporean context, the digital identity industry is much more reliant on the state as they do not have increased power due to the government being reliant on external expertise. Whereas the industry is a definitive stakeholder within the EU, within Singapore they are dependent stakeholders, only having urgency and legitimacy through coalitions such as ABS or SGTtech.

The Singaporean institutional context and large degree of policy competence effectively restrains corporate power, which alters lobbying strategies to be much more focused on showcasing alignment. In the European context, the fragmented nature and lack of expertise and capacity at the European Commission effectively empowers industry. Combined with the fact that through participation within LSPs they have gained a high degree of legitimacy, they can effectively act as co-legislators.

6. Conclusion

Comparing the institutional contexts of European Union and Singapore showcase that the lobbying strategies of the digital identity industry change depending upon the institutional context. In the European Union, lobbying actors have a higher degree of influence and access due to the dependence upon external expertise, as showcased in the reliance on LSPs. In Singapore, however, lobby strategies are centred around access to state-controlled infrastructure is seen as profitable and lobby strategies aimed at influencing the policy making process are largely abandoned.

6.1 Hypothesis 1

Due to the fragmentation and plurality of existing national identity infrastructure in the European Union and policy choices for a federated model in which actors compete for trust under regulatory guidelines, industry can behave as co-legislators. Through LSPs, a form of institutionalized lobby coalitions with high legitimacy, the digital identity industry can provide expertise and leverage that for economic benefits. Due to the high degree of complexity of the eIDAS 2.0 legislation, the lack of media attention and the fact that the main lobby of industry actors was regarding ensuring profitable business cases, little could be seen the strategy of mobilizing citizens to pressure policy makers and EU institutions. The first hypothesis, *"in decentralized institutional contexts that are dependent upon externally provided expertise, such as the European Union, lobbying actors will have a higher degree of influence and access in the policy making process."* is showcased to be true. However, as this is a case study consisting of only an analysis of the eIDAS 2.0 legislation, further research is needed to properly universalise and validate this hypothesis.

6.2 Hypothesis 2

In Singapore, however, due to a very high degree of centralization and governmental expertise, industry mainly focussed on accessing the wallet infrastructure. By aligning themselves with policy goals, such as the Smart Nation goals, they lobbied to become privileged partners as can be seen in the lobby around the MyInfo pilot for banks. Industry did not lobby to build the wallet or participate in its infrastructure with a profitable business case, rather they lobbied to integrate existing infrastructure within their own processes to optimize their customer acquisition and Know-Your-Customer obligations. As such, the second hypothesis, *"in highly centralized institutional contexts, with low dependence on externally provided expertise, such as Singapore, lobbying actors will have limited influence and access to the policy making process"* is partially true, as industry in Singapore primarily lobbies by showcasing alignment with policy goals. However, it is not possible to properly state that lobbying actors will not be able to gain more influence and access in future policy making processes. As with hypothesis 1, more validation is needed.

6.3 Main Research Question

As showcased throughout this thesis, lobbying strategies of the digital identity differ because of the type of technical implementation chosen (federated or state-controlled) and the institutional context. In Singapore, lobby is about alignment and access. In the European Union, lobby is about providing input for implementing acts through the LSPs that enable profitable business cases. The main research question "*how do the lobbying strategies of the digital identity industry differ between the Europe's eIDAS 2.0 implementation and Singapore's Singpass implementation and how can this be explained by institutional differences?"* has been answered by the application of the theoretical model on the case studies. The degree of centralisation and dependency on external expertise differ across institutional contexts, and fundamentally alter the lobbying goals and strategies of the digital identity industry.

The main goal of this thesis is to be descriptive, not to provide a normative answer as to which target architecture is better or which institutional context is more conducive to realizing public benefits.

However, it is concerning that the European Union will not only have, at the earliest, a wallet infrastructure 6 years later than Singapore, but also that this infrastructure is partially shaped by corporate actors driven by profit maximalization. A question worth asking to policymakers is whether the digital infrastructure of the future, that will be used for payment, travel, credentials, and much more, should have an architecture that enables profitable business cases.

6.4 Research Limitations

While researching and writing this thesis, various limitations quickly became apparent. In the research proposal, one goal was to supplement the document analysis with supplementary interviews. Sadly, however, my contacts in Singapore did not want to be formally interviewed. As such, there is no formal validation of the findings of this thesis by industry insiders. Due to time constraints and the lack of supplementary interviews from the Singaporean context, I decided to forgo the interviews for the European context. This limits the qualitative depth of this research.

There is also a mismatch between the scope of this research and the case studies found, as the digital identity industry is larger than just the example of payment processors provided. Whereas during my research I found multiple cases of lobby by platform providers such as Grab in Singapore or Amazon in the EU, they could not be properly cited or verified to be used as case studies in this research. As such, the usage of 'the digital identity industry' is somewhat disingenuous as all the examples of the case studies concern the payment processing industry, a subset of the originally intended scope.

The second limitation that became apparent is that Singapore is much less transparent than the EU, so obtaining relevant meeting minutes or other documents of the Singaporean government collaborating with private actors was difficult. The scope of this study is also on describing the different lobby strategies of the digital identity industry in different contexts, rather than proving actual influence on policy development or implementation. Some focus will, of course, be given on the success of these lobby strategies within each lobby context but the aim is not to prove the success of the lobby strategy. As such, proving direct causality remains firmly out of scope for this research, due to both the lack of transparency in Singapore and the descriptive approach of this research.

Thirdly, as the eIDAS 2.0 legislation is still in the implementation phase and the lobbying around the implementing acts is still ongoing, this thesis only gives a snapshot of the current process and cannot give a final description of the lobbying around the eIDAS 2.0 legislation.

My personal involvement in the implementation of the eIDAS 2.0 legislation could also be a limitative factor, as it could alter my neutrality and objectivity.

6.5 Further Research

Whereas further research regarding the lobby surrounding eIDAS 2.0 and Singpass would be interesting in order to validate these findings, these case studies are just one example of a comparative analysis.

As stated in the conclusion, the hypothesis formulated and the theoretical model need more validation with either a larger amount of case studies or a qualitative research approach.

Further research could generalize more and provide a more comprehensive analysis of institutional context and how it relates to potential lobby routes. The field of comparative public administration is still young and there are many more potential case studies that could provide valuable insights into the workings of different governments and provide transparency regarding the lobby activities of big multinational corporations. The geographical scope of this research could be expanded to include countries such as the USA or China, or instead of studying the lobbying around wallet-infrastructure, it could extend to general industry lobby.

Attempting to prove the success of various lobbying strategies and the causality of lobbying in relation to policy change across institutional contexts. There are plenty of avenues to add to the field of comparative public administration.

7. Bibliography

Academic Sources

Aoki, N. (2015). Let's Get Public Administration Right, But in What Sequence?: Lessons from Japan and Singapore. *Public Administration and Development*, 35(3), 206–218.

Binderkrantz, A. S., & Pedersen, H. H. (2024). Routes of access and influence. In *Research Handbook on Public Affairs* (pp. 192-205). Edward Elgar Publishing.

Bruycker, I. D., & Beyers, J. (2019). Lobbying strategies and success: Inside and outside lobbying in European Union legislative politics. *European Political Science Review*, 11(1), 57–74.

Choi, S.-J., Jia, N., & Lu, J. (2015). The Structure of Political Institutions and Effectiveness of Corporate Political Lobbying. *Organization Science*, *26*(1), 158-179.

Chua, L. J. (2012). Pragmatic Resistance, Law, and Social Movements in Authoritarian States: The Case of Gay Collective Action in Singapore. *Law & Society Review*, 46(4), 713–748.

Coen, D. (2007). Empirical and theoretical studies in EU lobbying. *Journal of European Public Policy*, 14(3), 333–345.

Coen, D., Katsaitis, A., & Vannoni, M. (2024). Lobbying in the European Union: Multi-venue and multi-actor strategies in the European Union. In *Handbook on Lobbying and Public Policy* (pp. 271–285). Edward Elgar Publishing.

De Bruycker, I. (2016). Pressure and Expertise: Explaining the Information Supply of Interest Groups in EU Legislative Lobbying. *JCMS: Journal of Common Market Studies*, 54(3), 599–616.

Degen, K., & Teubner, T. (2024). Wallet wars or digital public infrastructure? Orchestrating a digital identity data ecosystem from a government perspective. *Electronic Markets*, 34(1), 50.

Gorwa, R., Lechowski, G., & Schneiß, D. (2024). Platform lobbying: Policy influence strategies and the EU's Digital Services Act. *Internet Policy Review*, 13(2).

Guo, C., & Zhang, Z. (2014). Understanding nonprofit advocacy in non-Western settings: A framework and empirical evidence from Singapore. *VOLUNTAS*, 25(5).

Hillman, A. J., & Hitt, M. A. (1999). Corporate Political Strategy Formulation: A Model of Approach, Participation, and Strategy Decisions. *Academy of Management Review*, 24(4), 825–842.

Jreisat, J. (2011). *Globalism and Comparative Public Administration*. Routledge.

Kanol, D. (2024). The political system and cultural conditions: A comparative perspective. In *Research Handbook on Public Affairs* (pp. 85-98). Edward Elgar Publishing.

Klüver, H. (2011). The contextual nature of lobbying: Explaining lobbying success in the European Union. *European Union Politics*, *12*(4), 483-506.

Klüver, H., Braun, C., & Beyers, J. (2015a). Legislative lobbying in context: Towards a conceptual framework of interest group lobbying in the European Union. *Journal of European Public Policy*, *22*(4), 447-461.

Klüver, H., Braun, C., & Beyers, J. (2015b). Legislative lobbying in context: Towards a conceptual framework of interest group lobbying in the European Union. *Journal of European Public Policy*, *22*(4), 447-461.

Klüver, H., Braun, C., & Beyers, J. (2015). Legislative lobbying in context: Towards a conceptual framework of interest group lobbying in the European Union. *Journal of European Public Policy*, 22(4), 447–461.

Lee, E. W. Y., & Haque, M. S. (2006). The New Public Management Reform and Governance in Asian NICs: A Comparison of Hong Kong and Singapore. *Governance*, 19(4), 605–626.

Littoz-Monnet, A. (2014). The role of independent regulators in policy making: Venue-shopping and framing strategies in the EU. *European Journal of Political Research*, 53(1), 1–17.

Mahoney, C. (2008). Brussels Versus the Beltway: Advocacy in the United States and the European Union. Georgetown University Press.

Mitchell, N. J., Hansen, W. L., & Jepsen, E. M. (1997). The Determinants of Domestic and Foreign Corporate Political Activity. *The Journal of Politics*.

Mitchell, R. K., Agle, B. R., & Wood, D. J. (1997). Toward a theory of stakeholder identification and salience. *Academy of Management Review*, 22(4), 853–886.

Ortmann, S. (2012). Policy Advocacy in a Competitive Authoritarian Regime: The Growth of Civil Society and Agenda Setting in Singapore. *Administration & Society*, 44(6_suppl), 13S-25S.

Painter, M. (2004). The Politics of Administrative Reform in East and Southeast Asia: From Gridlock to Continuous Self-Improvement? *Governance*, 17(3), 361–386.

Ramírez, C. D., & Tan, L. H. (2004). Singapore Inc. Versus the Private Sector: Are Government-Linked Companies Different? *IMF Staff Papers*, 2004(003).

Sabatier, P. A. (1998). The advocacy coalition framework: Revisions and relevance for Europe. *Journal of European Public Policy*, 5(1), 98–130.

Vining, A. R. (2005). Building the firm's political (lobbying) strategy. *Journal of Public Affairs*, 5(2), 150–175.

Weymouth, S. (2012). Firm lobbying and influence in developing countries: A

multilevel approach. Business and Politics, 14(4), 1-26.

World Bank. (2022). National Digital Identity and Government Data Sharing in Singapore. Washington, DC. https://doi.org/10.1596/38201

Articles & Industry Reports

Apple Inc. (2025). Apple introduces Digital ID, a new way to create and present an ID in Apple Wallet. Apple Newsroom. https://www.apple.com/newsroom/2025/11/apple-introduces-digital-id-a-new-way-to-create-and-present-an-id-in-apple-wallet/

Aptitude. (n.d.). Aptitude - For European Digital Identity. https://aptitude.digital-identity-wallet.eu/

Biometric Update. (2025). The EUDI Wallet 'needs a sustainable business model'. https://www.biometricupdate.com/202510/the-eudi-wallet-needs-a-sustainable-business-model

Constantin. (2023). European industry associations call for payments in the Digital Identity Regulation to be non-mandatory. WSBI ESBG. https://www.wsbi-esbg.org/european-industry-associations-call-for-payments-in-the-digital-identity-regulation-to-be-non-mandatory/

Digital Credentials for Europe (DC4EU). (2025). DC4EU: Testing complex attribute verification for life events. https://www.dc4eu.eu/

DiResta, R. (2025). Lessons from National Digital ID Systems for Privacy, Security, and Trust in the AI Age. Tech Policy Press. https://techpolicy.press/lessons-from-national-digital-id-systems-for-privacy-security-and-trust-in-the-ai-age

EU Digital Identity Wallet Consortium (EWC). (2023). Members. https://eudiwalletconsortium.org/about-us/members/

European Commission. (2020a). Public consultation on the EU digital ID scheme for online transactions across Europe. https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/12528-EU-digital-ID-scheme-for-online-transactions-across-Europe/public-consultation_en

European Commission. (2020b). State of the Union 2020. https://commission.europa.eu/strategy-and-policy/state-union/state-union-2020_en

European Commission. (2025). EU Digital Identity Wallet Home and Pilot implementation. https://ec.europa.eu/digital-building-blocks/sites/spaces/EUDIGITALIDENTITYWALLET/pages/694487738/EU+Digital+Identity+Wallet+Home

European Council (2024). Implementing and delegated acts. https://www.consilium.europa.eu/en/council-eu/decision-making/implementing-and-delegated-acts/

Government Technology Agency of Singapore (GovTech). (2017). Opening Bank Accounts Becomes More Seamless and Convenient for MyInfo Users. https://www.tech.gov.sg/media/opening-bank-accounts-becomes-more-seamless-and-convenient-for-myinfo-users/

Government Technology Agency of Singapore (GovTech). (2021). Refreshed Singpass reflects improved services and drives digital innovations with private sector. https://www.tech.gov.sg/media/2021-03-04-refreshed-singpass/

Government Technology Agency of Singapore (GovTech). (n.d.). Our story and mission. https://www.tech.gov.sg/about-us/our-journey/our-story/

Information and Media Development Authority (IMDA). (2018). Media factsheet on Singpass National Digital Identity. https://isomer-user-content.by.gov.sg/38/f1b20296-6d5f-4ab9-8af9-2e503ec014d6/media%20factsheet%20on%20singpass%20national%20digital%20identity.pdf

iProov. (2020). Singapore Government Extends National Digital Identity programme. https://www.iproov.com/press/singapore-government-digital-identity

ITNews Asia (2021). Taiwan's Eva Air trials Affinidi's digital verification solution for COVID-19 tests. https://www.itnews.asia/news/taiwans-eva-air-trials-affinidis-digital-verification-solution-for-covid-19-tests-562955

Juniper Research. (2025). Digital wallet users to exceed 5.2 billion globally by 2026. https://www.juniperresearch.com/research/fintech-payments/core-payments/digital-wallet-research-report/

Lehmann, A., & socialhack. (2024). EU's Digital Identity Systems—Reality Check and Techniques for Better Privacy. CCC Video recording. https://media.ccc.de/v/38c3-eu-s-digital-identity-systems-reality-check-and-techniques-for-better-privacy

LSP-POTENTIAL. (2025). LSP-POTENTIAL - EU Digital Identity Wallet. https://ec.europa.eu/digital-building-blocks/sites/spaces/EUDIGITALIDENTITYWALLET/pages/924976339/LSP-POTENTIAL

Namirial. (2024). Understanding the Implementing Acts for EU Regulation 2024/1183 (eIDAS 2.0). https://www.namirial.com/en/blog/trust/understanding-the-implementing-acts-for-eu-regulation-2024-1183-eidas-2-0/

NOBID Consortium. (2025). Welcome to the NOBID Consortium—EUDIW. https://www.nobidconsortium.com/

OpenSSF. (2023). OpenSSF Co-Signs Industry Joint Statement on Article 45 in the EU's eIDAS Regulation. https://openssf.org/blog/2023/11/02/openssf-co-signs-industry-joint-statement-on-article-45-in-the-eus-eidas-regulation/

Prime Minister's Office (PMO) Singapore. (2017). Press Statement—Formation of the Smart Nation and Digital Government Group in PMO.

Regulation (EU) 2024/1183. (2024). Amending Regulation (EU) No 910/2014 as regards establishing the European Digital Identity Framework. https://eur-lex.europa.eu/eli/reg/2024/1183/oj

Rico, D. (2023). European Credit Sector Associations call for removing payments from the scope of the Digital Identity Regulation. EBF. https://www.ebf.eu/ebf-media-centre/european-credit-sector-associations-call-for-removing-payments-from-the-scope-of-the-digital-identity-regulation/

SGTech. (2022). Digital Trust Whitepaper.

SGTech. (2025). SGTech Web - Member Directory and Board of Governors. https://www.sgtech.org.sg/boardofGovernors

Signicat. (2025a). The elephant in the European Digital Identity Wallet room – how can actors get paid? https://www.signicat.com/blog/the-elephant-in-the-european-digital-identity-wallet-room-how-can-actors-get-paid

Signicat. (2025b). EU Commission Selects WE BUILD for Large-Scale Digital Identity Wallet Pilot. https://www.signicat.com/press-releases/ec-selects-we-build-for-large-scale-digital-identity-wallet-pilot

Singpass. (2025). Singpass Pricing Model and Service Level Subscription FAQ for Private Organisations. https://partnersupport.singpass.gov.sg/hc/en-sg/articles/34880999253145-Singpass-Pricing-Model-and-Service-Level-Subscription-FAQ-for-Private-Organisations

Temasek. (2025). Our T2030 Strategy and Holistic Identity via Affinidi. https://www.temasek.com.sg/en/about-us/our-t2030-strategy

Thoughtworks. (2025). Legacy modernization in the public sector. https://www.thoughtworks.com/en-in/clients/govtech

Thunes. (2025). Why mobile wallets are skyrocketing in emerging markets. https://www.thunes.com/insights/trends/why-mobile-wallets-are-skyrocketing-in-emerging-markets/

WE Build Consortium. (2025). WE BUILD Consortium - Business and Payment. https://www.webuildconsortium.eu/

8. Appendix I: internal documents

Some of the documents used for analysis are difficult to cite, as they are primarily internal documents and press releases gathered throughout this research. These documents have been added below.

Potential
For European Digital Identity

Co-funded by the European Union

POTENTIAL Pilot Concludes, Setting the Stage for Europe's Digital Identity Wallets

Press release, 29 September 2025

More than two years of EU-wide testing confirm that Europe's digital identity wallets can work securely across borders – if backed by common standards, strong governance, and citizen trust.

The POTENTIAL Large-Scale Pilot, one of four flagship initiatives under the Digital Europe Programme, has successfully concluded, marking a decisive step toward the deployment of the European Digital Identity Wallet (EUDI Wallet).

Over the past two years, more than 140 organisations from 19 Member States and Ukraine validated wallet use in six key areas: e-Government services, bank account opening, SIM card registration, mobile driving licence (mDL), qualified electronic signatures (QES), and e-prescriptions. In total, more than 1,300 tests and over 1,000 successful transactions — including 249 cross-border — were completed, confirming technical feasibility and providing essential insights for policy and governance.

"POTENTIAL has proven that Europe can achieve cross-border interoperability, but only if we apply common standards rigorously. Security is not just about technology — it requires governance, certification, and liability. And above all, citizens' trust will depend on wallets that are simple, transparent, and designed with privacy at their core. Looking ahead, the lessons of POTENTIAL will guide the transition from pilots to production, ensuring that the wallets will be secure, interoperable, and trusted across Europe," said Florent Tournois, Coordinator of the POTENTIAL project.

Key Results

The project delivered a functioning cross-border testing infrastructure, developed reusable attestations, validated wallet use in sensitive sectors such as health and banking, and delivered essential lessons for governance, interoperability and the security framework. These contributions will shape the European Commission's work on the Architecture and Reference Framework (ARF), the Reference Implementation (RI), and upcoming Implementing Acts under eIDAS 2.0.

Key Insights and Recommendations

The pilot generated a set of insights and recommendations for governments and policymakers. First, interoperability across borders is achievable but fragile, making EU-wide conformance testing and alignment with common standards essential. Second, governance is as critical as technology: Member States with strong national coordination and early private-sector engagement advanced fastest. Third, security depends not only on technical measures but also on robust governance, certification, and liability frameworks. Fourth, citizens' trust will require wallets that are simple, transparent, and privacy-preserving. Finally, inclusivity is key: smaller Member States and Ukraine benefitted from shared expertise but will need continued EU support to deploy at the same pace.

Looking Ahead

Between 2026 and 2027, Member States are expected to roll out national EUDI Wallets. The lessons of POTENTIAL provide a roadmap for success: accelerate alignment with ARF and eIDAS, establish strong governance structures, require conformance testing, and prioritise citizen-centric design and communication. Thanks to the groundwork laid by POTENTIAL, Europe is now better positioned to deliver digital identity wallets that are secure, interoperable, and trusted across the Union.

FORMATION OF THE SMART NATION AND DIGITAL GOVERNMENT GROUP IN THE PRIME MINISTER'S OFFICE

Since the Smart Nation initiative was launched in late 2014, progress has been made in applying digital and smart solutions to provide better services for our citizens and businesses. Companies have also responded with innovative products.

2. To enable the Government to be more integrated and responsive in our strategy and processes for Smart Nation and Digital Government (SNDG), the following organisational changes will take effect from **1 May 2017**:

a. The **Smart Nation and Digital Government Office (SNDGO)** will be formed under the Prime Minister's Office (PMO) comprising staff from the *Digital Government Directorate* of the Ministry of Finance (MOF), the *Government Technology Policy* department in the Ministry of Communications and Information (MCI), and the *Smart Nation Programme Office* (SNPO) in the PMO.

b. The *Government Technology Agency* (GovTech), a statutory board under MCI, will be placed under the PMO as the implementing agency of SNDGO.

3. Collectively, the SNDGO and GovTech will form the **Smart Nation and Digital Government Group (SNDGG)** in the Prime Minister's Office. Figure 1 [below] illustrates these organisational changes.

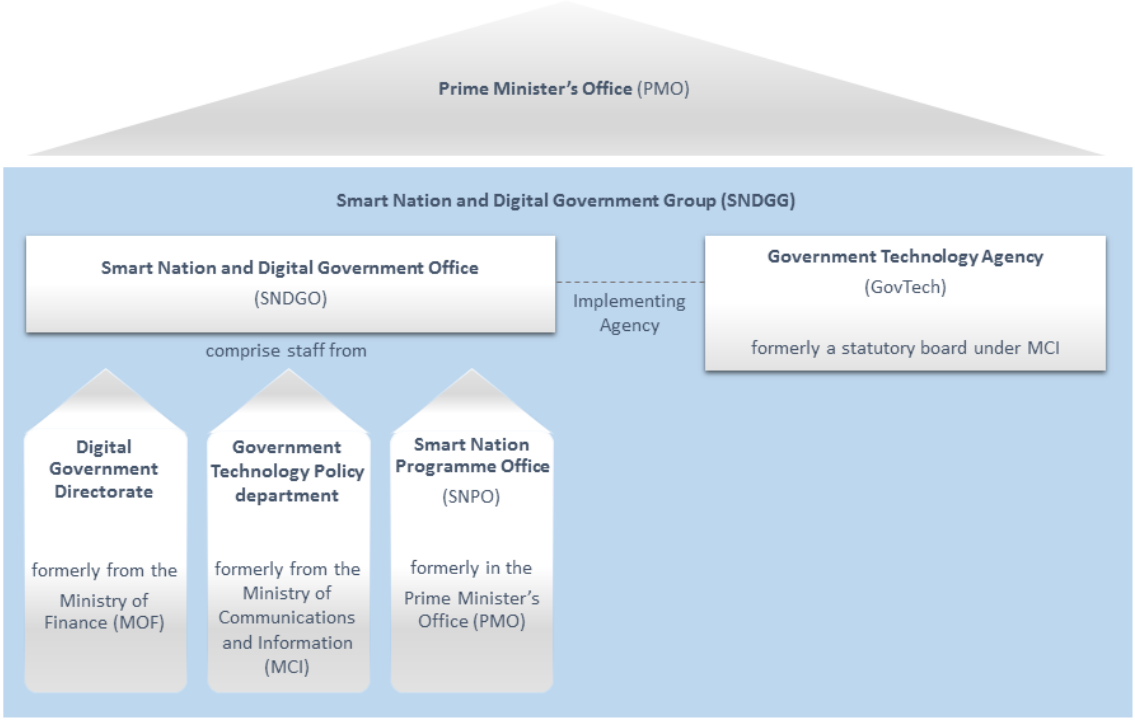


Figure 1: Organisational chart for Smart Nation and Digital Government Group (SNDGG) in the Prime Minister's Office

4. The SNDGG shall be responsible for the following:

a. **Apply digital and smart technologies to improve citizens' lives in key domains, in partnership with other government agencies, industry, and the public.** One such key domain is urban mobility. The Land Transport Authority (LTA) has been using data analytics to better manage our bus fleets, reduce crowdedness and improve timeliness. It has also been experimenting with self-driving vehicle technologies. The SNDGG will work with LTA to further exploit existing and emerging technologies to improve public transport, enhance urban logistics and reduce congestion so as to enhance the commuter experience;

b. **Develop the digital enablers and platforms for Smart Nation, to grow economic value and catalyse innovation by companies and citizens.** The SNDGG will build on the ongoing work by GovTech to enhance data sharing through data.gov.sg, and partner the Monetary Authority of Singapore (MAS) to promote e-payments.

The SNDGG will also drive the development of a national digital identity framework to facilitate digital transactions, and a national sensor communication backbone (the Smart Nation Platform) to support agencies' use of Internet of Things (IoT) applications to fulfil their missions.

c. **Drive digital transformation for the public service, to strengthen Government ICT infrastructure and improve public service delivery.** The SNDGG will build up digital capabilities within Government, including in areas such as data science and IoT, to continue delivering excellent public services to our citizens.

5. The SNDGG will be overseen by a Ministerial Committee chaired by Deputy Prime Minister (DPM) Teo Chee Hean. Dr Yaacob Ibrahim, Minister for Communications and Information will be Deputy Chairman and Minister-in-charge of Cybersecurity and the Info-communications Media Development Authority of Singapore (IMDA). The other members of the Ministerial Committee are Dr Vivian Balakrishnan, Minister-in-charge of the Smart Nation Initiative; Minister Ong Ye Kung, who has been appointed to champion Public Service innovation; and Minister of State Dr Janil Puthucheary, who will be the Minister-in-charge of GovTech and who will also coordinate GovTech's strategy with IMDA's industry development efforts.

6. Mr Ng Chee Khern, currently Permanent Secretary (PS) (Defence Development) of the Ministry of Defence (MINDEF), will concurrently lead the SNDG Group as the PS (Smart Nation and Digital Government). Mr Ng will also retain his appointment as the Chairman of the GovTech Board.

PRIME MINISTER'S OFFICE
SINGAPORE
20 MARCH 2017

ANNEX

A. Ministerial Quotes [for reporting]

Deputy Prime Minister (DPM) Teo Chee Hean "The establishment of the Smart Nation and Digital Government Group will strengthen our organisational ability to plan ahead, focus resources, orchestrate inter-agency efforts, and maintain a tight linkage between planning and implementation. This change is necessary to drive the Smart Nation initiative more effectively and to exploit the increasing opportunities offered by the accelerating pace of change in digital technology, and the increasing breadth and complexity of IT and smart systems."
Dr Yaacob Ibrahim, Minister for Communications and Information "I fully support the establishment of the Smart Nation Digital Government Group, with GovTech moving to the Prime Minister's Office. This will build on the strong foundation laid by MCI when we established GovTech last October, and boost the public sector's digital transformation efforts. To realise our vision of a Smart Nation, we also need a thriving digital economy, a digitally-savvy population and a secure cyber space. MCI, IMDA and CSA will continue to work with the industry and our workers, to build a cyber-secure nation and seize the opportunities in the digital economy."
Dr Vivian Balakrishnan, Minister-in-charge of the Smart Nation Initiative "Over the next year, I hope to see major progress in three signature programmes – Digital Identity, E-Payments and a national IOT/sensors system that will provide synergies for all government agencies and expand opportunities for the private sector. By consolidating GovTech and the various policy, planning and implementing agencies together in PMO, we will be able to quickly and decisively roll out these digital platforms for our citizens and businesses. These platforms are foundational to the building of a Smart Nation. They will expand job opportunities and enable our citizens and businesses to innovate and create economic value in the new digital economy."

B. Supplementary Information

About Ministry of Finance's Digital Government Directorate:

The Digital Government Directorate (DGD) supports the Ministry of Finance's (MOF) strategic outcome of building a high performance government. DGD works in partnership with other agencies to advance digitalisation initiatives in the Public Sector through the active use of technology, data and design so as to enhance service delivery to the public. DGD's functions include:

a. Central ICT Platforms – Own and manage Whole-of-Government ICT platforms used by individuals and businesses, such as SingPass, CorpPass, MyInfo, data.gov.sg and the CitizenConnect Centres

b. Digital Services Strategy – Design and implement digital service strategies that improve service delivery to the public

c. Data Policy and Governance – Develop policies on the sharing and protection of public sector data

d. ICT Resource Governance – Ensure that the Public Sector is efficient and effective in its use of ICT resources

About Ministry of Communications and Information's Government Technology Policy Department:

The Ministry of Communications and Information's (MCI) Government Technology Policy department designs and reviews policies to:

a. Make the Government's ICT systems and infrastructure more innovative, user-friendly, secure and resilient

b. Deepen the Government's ICT engineering capabilities

c. Strengthen the Government's ICT governance standards

About Smart Nation Programme Office

The Smart Nation Programme is a multi-agency initiative to enhance quality of life, create economic opportunities and build stronger community bonds, through the effective development, deployment and use of digital technology and networks.

The Smart Nation Programme Office (SNPO) drives this whole-of-government endeavour. Its key roles are:

a. Coordinate key Smart Nation initiatives by various agencies, in areas that significantly impact citizens and businesses

b. Oversee development of cross cutting enablers that facilitate widespread technology innovation, in government, industry and community

c. Facilitate the involvement and engagement of citizens and companies in designing, building and using digital solutions

About Government Technology Agency of Singapore

The Government Technology Agency of Singapore (GovTech) is a statutory board formed in October 2016 after the restructuring of the Infocomm Development Authority. GovTech works with public agencies to develop and deliver secure digital services and applied technology to individuals and businesses in Singapore. GovTech builds key platforms and solutions needed to support Singapore as a Smart Nation. As a leading centre for information communications technology and related engineering such as the Internet of Things, GovTech also enhances the capabilities of the Singapore Government in these domains.

For media clarifications, please contact:

Mr Wong Ruqin
Manager, Smart Nation Programme Office, PMO
Tel: +6592294450
Email: Wong_Ruqin@snpo.gov.sg

Mr Tan Boon Leng
Manager, Communications and Marketing Group, GovTech
Tel: +6562110375
Email: Tan_Boon_Leng@tech.gov.sg

Potential
For European Digital Identity

Co-funded by the European Union

POTENTIAL Pilot Concludes, Setting the Stage for Europe's Digital Identity Wallets

Press release, 29 September 2025

More than two years of EU-wide testing confirm that Europe's digital identity wallets can work securely across borders – if backed by common standards, strong governance, and citizen trust.

The POTENTIAL Large-Scale Pilot, one of four flagship initiatives under the Digital Europe Programme, has successfully concluded, marking a decisive step toward the deployment of the European Digital Identity Wallet (EUDI Wallet).

Over the past two years, more than 140 organisations from 19 Member States and Ukraine validated wallet use in six key areas: e-Government services, bank account opening, SIM card registration, mobile driving licence (mDL), qualified electronic signatures (QES), and e-prescriptions. In total, more than 1,300 tests and over 1,000 successful transactions — including 249 cross-border — were completed, confirming technical feasibility and providing essential insights for policy and governance.

"POTENTIAL has proven that Europe can achieve cross-border interoperability, but only if we apply common standards rigorously. Security is not just about technology — it requires governance, certification, and liability. And above all, citizens' trust will depend on wallets that are simple, transparent, and designed with privacy at their core. Looking ahead, the lessons of POTENTIAL will guide the transition from pilots to production, ensuring that the wallets will be secure, interoperable, and trusted across Europe," said Florent Tournois, Coordinator of the POTENTIAL project.

Key Results

The project delivered a functioning cross-border testing infrastructure, developed reusable attestations, validated wallet use in sensitive sectors such as health and banking, and delivered essential lessons for governance, interoperability and the security framework. These contributions will shape the European Commission's work on the Architecture and Reference Framework (ARF), the Reference Implementation (RI), and upcoming Implementing Acts under eIDAS 2.0.

Key Insights and Recommendations

The pilot generated a set of insights and recommendations for governments and policymakers. First, interoperability across borders is achievable but fragile, making EU-wide conformance testing and alignment with common standards essential. Second, governance is as critical as technology: Member States with strong national coordination and early private-sector engagement advanced fastest. Third, security depends not only on technical measures but also on robust governance, certification, and liability frameworks. Fourth, citizens' trust will require wallets that are simple, transparent, and privacy-preserving. Finally, inclusivity is key: smaller Member States and Ukraine benefitted from shared expertise but will need continued EU support to deploy at the same pace.

Looking Ahead

Between 2026 and 2027, Member States are expected to roll out national EUDI Wallets. The lessons of POTENTIAL provide a roadmap for success: accelerate alignment with ARF and eIDAS, establish strong governance structures, require conformance testing, and prioritise citizen-centric design and communication. Thanks to the groundwork laid by POTENTIAL, Europe is now better positioned to deliver digital identity wallets that are secure, interoperable, and trusted across the Union.

ANNEX B

Quotes from participating banks

Ms Susan Hwee, Head, Group Technology and Operations, UOB
"Our customers already enjoy paperless account opening in the branch. With MyInfo, new customers will enjoy faster time-to-approval as forms are auto-populated with a person's verified details. The convenience of MyInfo further builds and leverages on our digital infrastructure; removing the need for customers to scan and submit supporting documents when opening a UOB bank account online."

Mr Jeremy Soo, Head, Consumer Banking Group (Singapore), DBS Bank
"The seamlessness of MyInfo brings us one step closer to our shared vision of a Smart Nation. Customers will enjoy a simpler, easier application process, reducing an estimated 80 per cent of the average time taken to fill in an application. MyInfo will also complement our suite of digital services, where customers are conducting some 60 million transactions via DBS/POSB internet and mobile banking every month."

Mr Ching Wei Hong, Chief Operating Officer, OCBC Bank
"Data is the fuel of the economy, and as Singapore accelerates the creation of a Smart Nation, how data is shared, how easily it flows and how it can be used securely with user consent will determine Singapore's progress and economic performance. The MyInfo platform will enable us to offer customers even more products and services digitally, and leapfrog us into a future of paperless banking."

Dr Michael Gorriz, Group Chief Information Officer, Standard Chartered Bank
"Standard Chartered is on our way to being a digital bank with a human touch. Looking at solutions from our customers' view, we want to make banking digital, convenient and secure so customers can enjoy easy and seamless experiences. We are proud to be the first global bank to partner with GovTech to bring this ground-breaking MyInfo innovation to our customers in Singapore."

tech.gov.sg

GOVERNMENT TECHNOLOGY AGENCY
10 Pasir Panjang Road #10-01
Mapletree Business City, Singapore 117438
T +65 6211 0888
E info@tech.gov.sg

A SMART NATION FOR A FUTURE-READY SINGAPORE

Factsheet – SingPass, Singapore's national digital identity

Overview

SingPass, Singapore's national digital identity, is one of the Smart Nation strategic national projects. As a foundational digital infrastructure, the national digital identity is critical to achieving our vision of improving lives of citizens, creating opportunities for businesses, and transforming the capabilities of government agencies.

Today, there are more than 4 million SingPass users. SingPass enables access to over 1,400 digital services by 340 government agencies and private organisations. Over 170 million transactions are conducted using SingPass annually.

The current suite of services includes SingPass Mobile app, MyInfo, MyInfo Business, Login, Verify, Face Verification, Sign and Notify. Remote authorisation of transactions will be available by end of the year. Companies interested in using these services can visit the NDI Developer and Partner Portal at https://www.ndi-api.gov.sg.

SingPass Features and Services

SingPass Mobile app

The SingPass Mobile app was launched in October 2018 to provide greater convenience when users access government and private sector services online and in person. Users can check their CPF balance, apply for HDB flats, perform internet banking or manage their insurance policies with ease, without having to remember passwords.

Popular features include login shortcuts to frequently-used government digital services and a customisable profile for personal information at a glance. The latest Face Verification feature lets overseas users set up their SingPass Mobile app easily, doing away with the need for a Singapore mobile number. Users can also digitally sign electronic documents such as applications for insurance policies using their SingPass Mobile app.

As of February 2021, there are more than 2.4 million SingPass Mobile users. More than 70% of all SingPass transactions are conducted through the app, with the remaining 30% using Two-Factor Authentication (2FA) methods like SMS-OTP.

MyInfo

MyInfo enables users to pre-fill digital forms with their personal data from government sources for online transactions, while giving them control over how their information is shared.

To date, close to 600 digital services offered by government agencies and businesses have been on-boarded to MyInfo. Since then, the use of MyInfo has resulted in an average decrease of up to 80 per cent in application time for users, with businesses reporting up to 15 per cent higher approval rate due to better data quality and significant cost savings in their customer acquisition process. This service sees more than 200,000 transactions a day.

MyInfo Business

Similar to MyInfo, MyInfo Business enables businesses to pre-fill digital forms with entity data from government sources, such as corporate profile, financial performance and ownership information. It facilitates 120 Government-to-Business (G2B) digital services such as applying for a grant on the Business Grants Portal and invoicing agencies on Vendors@Gov.

This service has also been extended to private sector services like opening of a corporate utilities account and application of SME loans. To date, there are 48 private sector digital services from 15 organisations on-boarded to MyInfo Business.

Login

Businesses can tap on Login for authentication processes, while customers can do away with remembering one additional set of credentials. To date, there are more than 50 private sector organisations leveraging Login as an authentication gateway, including OCBC Bank, Prudential, NTUC Union, Income Insurance, Singapore Exchange, the Singapore Employers' Federation and JustLogin's HR software.

Verify

Verify enables users to perform face-to-face identity verification and secure transfer of personal information through scanning of QR codes or Near-Field Communication (NFC). Using SingPass Mobile app, the user simply scans a QR code (e.g. at an event registration counter) and consents to have his basic personal details used in the transaction.

This feature is currently used at the GivePls platform for donor registrations and SingHealth Polyclinics for new patient registration, without the need for individuals to present or hand over their identity documents. Businesses that have face-to-face registration processes, such as real estate companies, healthcare institutions, financial institutions, automobile industry and training providers, have also expressed interest to use Verify.

Face Verification

Face Verification is an authentication method that enables users to access digital services on desktop or mobile browsers using a face scan that is compared against the Government's biometric database (such as their latest NRIC / Passport / Work Pass photo). This can be layered upon relying parties' existing authentication process to enable multi-factor authentication and provide a higher identity assurance, especially for transactions involving sensitive information or of higher transaction value.

The feature also improves digital inclusion, as it can be used by individuals who do not have mobile phones. This is being piloted for logins to government digital services at kiosks located at various agencies such as IRAS Taxpayer and Business Service Centre and Our Tampines Hub's Public Service Centre since April 2020, at selected public libraries since September 2020, and at all CPFB Service Centres since December 2020. More locations will be added progressively.

As of February 2021, over 19,000 users have accessed services at these kiosks through the face verification feature. Users who visit the service centres to reset their SingPass passwords

have also seen a reduction in waiting time of over 10 minutes as the technology offers improved convenience and ease of use.

Sign

Sign enables users to digitally sign documents using their SingPass Mobile app. Signing with SingPass provides convenience and increases productivity and business efficiency - citizens no longer need to be physically present to sign documents and agreements.

The user flow is similar to a SingPass login, as users simply scan the QR code displayed on the screen and authenticate themselves following the on-screen instructions. Sign with SingPass produces a digital signature that is cryptographically linked to the signer, which provides higher assurance of the authenticity and integrity of the signed documents. The digital signature can also be validated independently by other parties, enabling end-to-end digitalisation even for workflows that involve multiple organisations.

Businesses can choose to either integrate their document workflows directly with Sign API or use commercial document management products that are pre-integrated with Sign API. To date, there are eight digital signing application providers, namely DocuSign, iText, Netrust, Adobe, Onespan, Dedoco, Tessaract.io and Kofax. ERA Realty Network and AIA Singapore have begun piloting Sign for their business applications.

Notify

Notify sends users relevant and timely notifications from government agencies directly into their SingPass Mobile inbox. Through the notification, users can either view Government notices or log in seamlessly to the agency's digital service to complete their transactions.

Current examples include (i) SafeEntry Pass notifications which are sent to SingPass Mobile users who have performed their SafeEntry check-ins using the app, and (ii) NRIC re-registration and Passport renewal notifications, which are sent to the user's SingPass Mobile inbox, and (iii) SingapoRediscovers Vouchers deduction notifications, which are sent by the Singapore Tourism Board (STB) to the user's SingPass Mobile inbox. Transactional notifications such as Medisave deduction and payment reminders will be ready in 2021.

By accessing notifications through SingPass Mobile inbox, citizens can be assured that the messages are authentic and sent by government agencies, and mitigate the risks of phishing emails or text messages.

An Inclusive National Digital Identity System

Ensuring inclusion and widespread access by all residents is a key design of SingPass. We have therefore added features such as Face Verification and Multi-User SMS 2FA, to ensure that even users without mobile phones can use their digital identities to access digital services.

Face Verification can be used by any SingPass user who has access to an internet-device with a web camera or front-facing camera, including public kiosks as mentioned earlier.

The Multi-User SMS 2FA is an extension of the existing SMS-OTP 2FA method. Users – who may require the assistance of others when transacting online – can opt to have their SMS-

OTP sent to a trusted SingPass user's mobile number, for example of an immediate family member.

As there are alternative 2FA methods that ensure users are able to conveniently use SingPass, the OneKey token will be discontinued from 1 April 2021. OneKey token users have already been notified and prompted to set up their SingPass Mobile or other 2FA methods, or to use Face Verification which does not require any additional setup. For more information, OneKey users can visit http://go.gov.sg/singpass-2fa-methods which contains instructions on switching to these 2FA alternatives.

#####

SingPass – Singapore's national digital identity

Overview

Today, more than 4 million Singapore citizens and residents use SingPass, Singapore's national digital identity. A cornerstone of Singapore's Smart Nation initiative, the national digital identity ecosystem is critical in achieving Singapore's Smart Nation vision of delivering significant benefits to citizens and businesses, and transforming the capabilities of government agencies through digital platforms. SingPass, as a secured gateway, has evolved to allow access to over 1,000 digital services offered by some 250 government agencies and private organisations. Over 120 million transactions are conducted using SingPass annually.

This Smart Nation strategic national project brings convenience to the everyday lives of citizens, catalyses industry to develop more value-added services, and increases opportunities for government-to-citizen co-creation. Made available to the private sector to enhance their digital services, SingPass helps support Singapore's digital economy and our vision of a global ecosystem for interoperable national digital identities.

The current suite of services and features include SingPass Mobile, MyInfo, Login, Verify, Notify, Face Verification and Sign. Remote authorisation of transactions will be available in 2021.

SingPass Mobile

The SingPass Mobile app was launched in October 2018 to provide greater convenience when users access government and private sector services online and in person. Users can check their CPF balance, apply for HDB flats or manage their insurance policies with ease.

Popular features include login shortcuts to frequently-used government digital services and a customisable profile for personal information at a glance. The latest face verification feature supports easy onboarding by overseas users, doing away with the need for a Singapore mobile number.

As of November 2020, more than 2.1 million SingPass users are actively using SingPass Mobile to access services, with more than 60 per cent of all SingPass transactions conducted through the app.

MyInfo

MyInfo enables users to pre-fill digital forms with their personal data from government sources for online transactions, while giving them control over how their information is shared.

To date, close to 600 digital services offered by government agencies and businesses have been on-boarded to MyInfo. Since then, the use of MyInfo has resulted in an average decrease of up to 80 per cent in application time for users, with businesses reporting up to 15 per cent higher

GOVERNMENT TECHNOLOGY AGENCY
10 Pasir Panjang Road #10-01
Mapletree Business City, Singapore 117438
T +65 6211 0888
E info@tech.gov.sg

approval rate due to better data quality and significant cost savings in their customer acquisition process. This service sees more than 200,000 transactions a day.

MyInfo Business

MyInfo Business enables businesses to pre-fill digital forms with entity data from government sources for seamless Government to Business (G2B) and Business to Business transactions, such as corporate profile, financial performance and ownership information. It facilitates 118 G2B digital services such as applying for a grant on the Business Grants Portal and invoicing agencies on Vendors@Gov.

This service is being piloted with some private sector services for opening of a corporate utilities account and application of SME loans. Singapore-registered business owners can log in through CorpPass, give consent and have authorised data pre-filled in these participating digital services. To date, there are over 40 private sector digital services from 9 organisations on-boarded to MyInfo Business.

Login

Businesses can tap on Login for identity assurance and authentication processes, while customers can do away with remembering one additional set of credentials. To date, there are 40 private sector organisations leveraging Login as an authentication gateway, including OCBC Bank, Prudential, NTUC Union, Income Insurance, the Singapore Employers' Federation and JustLogin's HR software.

Verify

Verify enables users to perform secure face-to-face identity verification and data transfer through scanning of QR codes or Near-Field Communication (NFC). Using SingPass Mobile, the user simply scans a secure QR code at the counter and consents to have his basic personal details used in the transaction.

This feature is being piloted at Republic Plaza for visitor registration and Punggol Polyclinic for new patient registration, without the need for residents to present their identity documents. Businesses that have face-to-face registration processes, such as real estate companies, healthcare institutions, financial institutions, the automobile industry and training providers, have also expressed interest to integrate their services with Verify.

Face Verification

Face Verification enables users to access services on web or mobile browsers by comparing a person's presented facial image with the Government's biometric database (such as their latest NRIC / Passport / Work Pass photo). This can be layered upon relying parties' existing authentication process to enable multi-factor authentication and provide a higher identity assurance, especially for transactions involving sensitive information.

GOVERNMENT TECHNOLOGY AGENCY
10 Pasir Panjang Road #10-01
Mapletree Business City, Singapore 117438
T +65 6211 0888
E info@tech.gov.sg

The feature is being piloted for logins to government digital services at agencies' kiosks located at IRAS Taxpayer and Business Service Centre and Our Tampines Hub's Public Service Centre since April 2020, and CPFB's Bishan Service Centre since September 2020.

As of 1 October 2020, over 4,200 users have accessed services at these kiosks through the face scan feature. Users who visit the service centres to reset their SingPass passwords have also seen a reduction in waiting time of over 10 minutes.

Sign

Sign enables users to digitally sign documents using their SingPass Mobile app by scanning the QR code displayed on the screen before authenticating themselves. Sign employs technology to ensure the integrity of the signed document and to counter repudiation.

Businesses and services such as document signing applications can integrate and provide trusted signatures directly with SingPass, increasing trust and assurance with their existing document signing products. Signing with SingPass provides convenience, productivity and efficiency - citizens no longer need to be physically present to sign documents and agreements, and businesses can digitalise document verification and filing.

From November 2020, the collaboration with eight digital signing application providers, namely DocuSign, iText, Netrust, Adobe, Onespan, Dedoco, Tessaract.io and Kofax, will progressively be rolled out. The legal and financial sectors will first pilot Sign.

Notify

Notify sends users relevant and timely notifications from government agencies directly into their SingPass Mobile inbox. Through the inbox link, users can log in seamlessly to the agency's digital service to complete their necessary transactions.

Current examples include (i) SafeEntry Pass notifications which are sent to SingPass Mobile users who have performed their SafeEntry check-ins using the app, and (ii) NRIC and Passport renewal notifications, which are sent by the Immigration & Checkpoints Authority (ICA) to the user's SingPass Mobile inbox.

###

tech.gov.sg

GOVERNMENT TECHNOLOGY AGENCY
10 Pasir Panjang Road #10-01
Mapletree Business City, Singapore 117438
T +65 6211 0888
E info@tech.gov.sg

For media enquiries, please contact:

Medha Lim
Senior Manager, Communications and Marketing Group
GovTech
Email: Medha_LIM@tech.gov.sg

Lydia Lee
Manager, Communications and Marketing Group
GovTech
Email: Lydia_LEE@tech.gov.sg

Serene Chan
Assistant Manager, Communications and Marketing Group
GovTech
Email: Serene_CHAN@tech.gov.sg

FORMATION OF THE SMART NATION AND DIGITAL GOVERNMENT GROUP IN THE PRIME MINISTER'S OFFICE

Since the Smart Nation initiative was launched in late 2014, progress has been made in applying digital and smart solutions to provide better services for our citizens and businesses. Companies have also responded with innovative products.

2. To enable the Government to be more integrated and responsive in our strategy and processes for Smart Nation and Digital Government (SNDG), the following organisational changes will take effect from **1 May 2017**:

a. The **Smart Nation and Digital Government Office (SNDGO)** will be formed under the Prime Minister's Office (PMO) comprising staff from the *Digital Government Directorate* of the Ministry of Finance (MOF), the *Government Technology Policy* department in the Ministry of Communications and Information (MCI), and the *Smart Nation Programme Office* (SNPO) in the PMO.

b. The *Government Technology Agency* (GovTech), a statutory board under MCI, will be placed under the PMO as the implementing agency of SNDGO.

3. Collectively, the SNDGO and GovTech will form the **Smart Nation and Digital Government Group (SNDGG)** in the Prime Minister's Office. Figure 1 [below] illustrates these organisational changes.

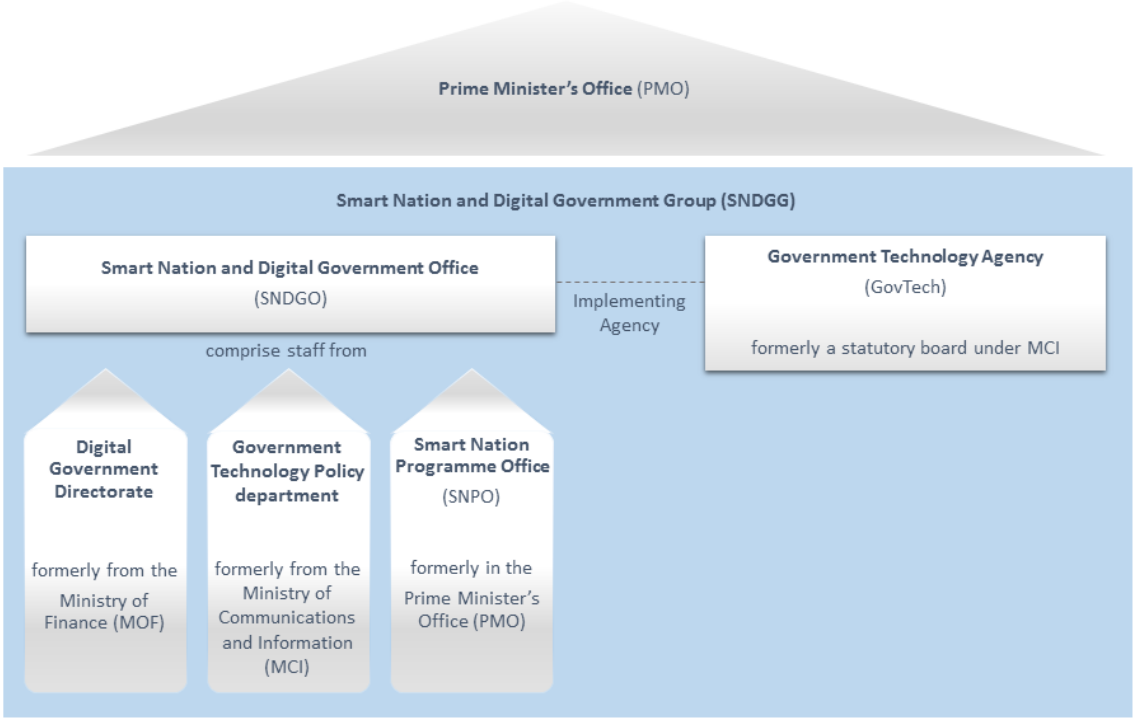


Figure 1: Organisational chart for Smart Nation and Digital Government Group (SNDGG) in the Prime Minister's Office

4. The SNDGG shall be responsible for the following:

a. **Apply digital and smart technologies to improve citizens' lives in key domains, in partnership with other government agencies, industry, and the public.** One such key domain is urban mobility. The Land Transport Authority (LTA) has been using data analytics to better manage our bus fleets, reduce crowdedness and improve timeliness. It has also been experimenting with self-driving vehicle technologies. The SNDGG will work with LTA to further exploit existing and emerging technologies to improve public transport, enhance urban logistics and reduce congestion so as to enhance the commuter experience;

b. **Develop the digital enablers and platforms for Smart Nation, to grow economic value and catalyse innovation by companies and citizens.** The SNDGG will build on the ongoing work by GovTech to enhance data sharing through data.gov.sg, and partner the Monetary Authority of Singapore (MAS) to promote e-payments.

The SNDGG will also drive the development of a national digital identity framework to facilitate digital transactions, and a national sensor communication backbone (the Smart Nation Platform) to support agencies' use of Internet of Things (IoT) applications to fulfil their missions.

c. **Drive digital transformation for the public service, to strengthen Government ICT infrastructure and improve public service delivery.** The SNDGG will build up digital capabilities within Government, including in areas such as data science and IoT, to continue delivering excellent public services to our citizens.

5. The SNDGG will be overseen by a Ministerial Committee chaired by Deputy Prime Minister (DPM) Teo Chee Hean. Dr Yaacob Ibrahim, Minister for Communications and Information will be Deputy Chairman and Minister-in-charge of Cybersecurity and the Info-communications Media Development Authority of Singapore (IMDA). The other members of the Ministerial Committee are Dr Vivian Balakrishnan, Minister-in-charge of the Smart Nation Initiative; Minister Ong Ye Kung, who has been appointed to champion Public Service innovation; and Minister of State Dr Janil Puthucheary, who will be the Minister-in-charge of GovTech and who will also coordinate GovTech's strategy with IMDA's industry development efforts.

6. Mr Ng Chee Khern, currently Permanent Secretary (PS) (Defence Development) of the Ministry of Defence (MINDEF), will concurrently lead the SNDG Group as the PS (Smart Nation and Digital Government). Mr Ng will also retain his appointment as the Chairman of the GovTech Board.

PRIME MINISTER'S OFFICE
SINGAPORE
20 MARCH 2017

ANNEX

A. Ministerial Quotes [for reporting]

Deputy Prime Minister (DPM) Teo Chee Hean "The establishment of the Smart Nation and Digital Government Group will strengthen our organisational ability to plan ahead, focus resources, orchestrate inter-agency efforts, and maintain a tight linkage between planning and implementation. This change is necessary to drive the Smart Nation initiative more effectively and to exploit the increasing opportunities offered by the accelerating pace of change in digital technology, and the increasing breadth and complexity of IT and smart systems."
Dr Yaacob Ibrahim, Minister for Communications and Information "I fully support the establishment of the Smart Nation Digital Government Group, with GovTech moving to the Prime Minister's Office. This will build on the strong foundation laid by MCI when we established GovTech last October, and boost the public sector's digital transformation efforts. To realise our vision of a Smart Nation, we also need a thriving digital economy, a digitally-savvy population and a secure cyber space. MCI, IMDA and CSA will continue to work with the industry and our workers, to build a cyber-secure nation and seize the opportunities in the digital economy."
Dr Vivian Balakrishnan, Minister-in-charge of the Smart Nation Initiative "Over the next year, I hope to see major progress in three signature programmes – Digital Identity, E-Payments and a national IOT/sensors system that will provide synergies for all government agencies and expand opportunities for the private sector. By consolidating GovTech and the various policy, planning and implementing agencies together in PMO, we will be able to quickly and decisively roll out these digital platforms for our citizens and businesses. These platforms are foundational to the building of a Smart Nation. They will expand job opportunities and enable our citizens and businesses to innovate and create economic value in the new digital economy."

B. Supplementary Information

About Ministry of Finance's Digital Government Directorate:

The Digital Government Directorate (DGD) supports the Ministry of Finance's (MOF) strategic outcome of building a high performance government. DGD works in partnership with other agencies to advance digitalisation initiatives in the Public Sector through the active use of technology, data and design so as to enhance service delivery to the public. DGD's functions include:

a. Central ICT Platforms – Own and manage Whole-of-Government ICT platforms used by individuals and businesses, such as SingPass, CorpPass, MyInfo, data.gov.sg and the CitizenConnect Centres

b. Digital Services Strategy – Design and implement digital service strategies that improve service delivery to the public

c. Data Policy and Governance – Develop policies on the sharing and protection of public sector data

d. ICT Resource Governance – Ensure that the Public Sector is efficient and effective in its use of ICT resources

About Ministry of Communications and Information's Government Technology Policy Department:

The Ministry of Communications and Information's (MCI) Government Technology Policy department designs and reviews policies to:

a. Make the Government's ICT systems and infrastructure more innovative, user-friendly, secure and resilient

b. Deepen the Government's ICT engineering capabilities

c. Strengthen the Government's ICT governance standards

About Smart Nation Programme Office

The Smart Nation Programme is a multi-agency initiative to enhance quality of life, create economic opportunities and build stronger community bonds, through the effective development, deployment and use of digital technology and networks.

The Smart Nation Programme Office (SNPO) drives this whole-of-government endeavour. Its key roles are:

a. Coordinate key Smart Nation initiatives by various agencies, in areas that significantly impact citizens and businesses

b. Oversee development of cross cutting enablers that facilitate widespread technology innovation, in government, industry and community

c. Facilitate the involvement and engagement of citizens and companies in designing, building and using digital solutions

About Government Technology Agency of Singapore

The Government Technology Agency of Singapore (GovTech) is a statutory board formed in October 2016 after the restructuring of the Infocomm Development Authority. GovTech works with public agencies to develop and deliver secure digital services and applied technology to individuals and businesses in Singapore. GovTech builds key platforms and solutions needed to support Singapore as a Smart Nation. As a leading centre for information communications technology and related engineering such as the Internet of Things, GovTech also enhances the capabilities of the Singapore Government in these domains.

For media clarifications, please contact:

Mr Wong Ruqin
Manager, Smart Nation Programme Office, PMO
Tel: +6592294450
Email: Wong_Ruqin@snpo.gov.sg

Mr Tan Boon Leng
Manager, Communications and Marketing Group, GovTech
Tel: +6562110375
Email: Tan_Boon_Leng@tech.gov.sg

Digital Trust

Unlocking the Next Wave of Growth in the Digital Economy

SGTECH
WHERE TECH MEETS

Digital Trust

Unlocking the Next Wave of Growth in the Digital Economy

Published by

SGTECH
WHERE TECH MEETS

Presenting Sponsors

aws

NetSfere
Enabling Communication.

Supporting Sponsors

intel

Lenovo

Microsoft

Published in 2022 by SGTech
79 Ayer Rajah Crescent #02-03/04/05
Singapore 139955

research@sgtech.org.sg
www.sgtech.org.sg

Table of Contents

Wong Wai Meng
Chair, SGTech

Digitalisation offers new approaches to trust. Competitors who do not see eye-to-eye can still transact efficiently because technologies such as privacy-enhancing technologies, distributed ledgers (also called shared ledgers), coupled with good governance in processes now enable these interactions even without parties knowing who they transact with.

1 Preface by SGTech

Wong Wai Meng

Chair, SGTech

Trust is defined as a firm belief in the reliability, truth, ability, or strength of someone or something, one in which confidence is placed. Trust has always been the linchpin of strong relationships, especially between individuals and businesses. Digital Trust is the same thing but applied to digital technology.

The whitepaper that you are reading now captures the core findings of SGTech's Digital Trust Landscape Study. Interviews with over 80 local, regional, and global industry leaders in their respective fields were conducted to map out the landscape for Digital Trust.

Why is Digital Trust critical now? With the increasing merging of the physical, digital, and biological worlds, it has created huge opportunities but also challenges for the way we live and work. The advent of technologies such as blockchain, artificial intelligence, big data, internet of things, and many more, has accelerated the pace of innovation in business. Internal resources alone are no longer sufficient for addressing the dynamic needs of markets; companies must adopt innovation strategies by collaborating with external stakeholders.

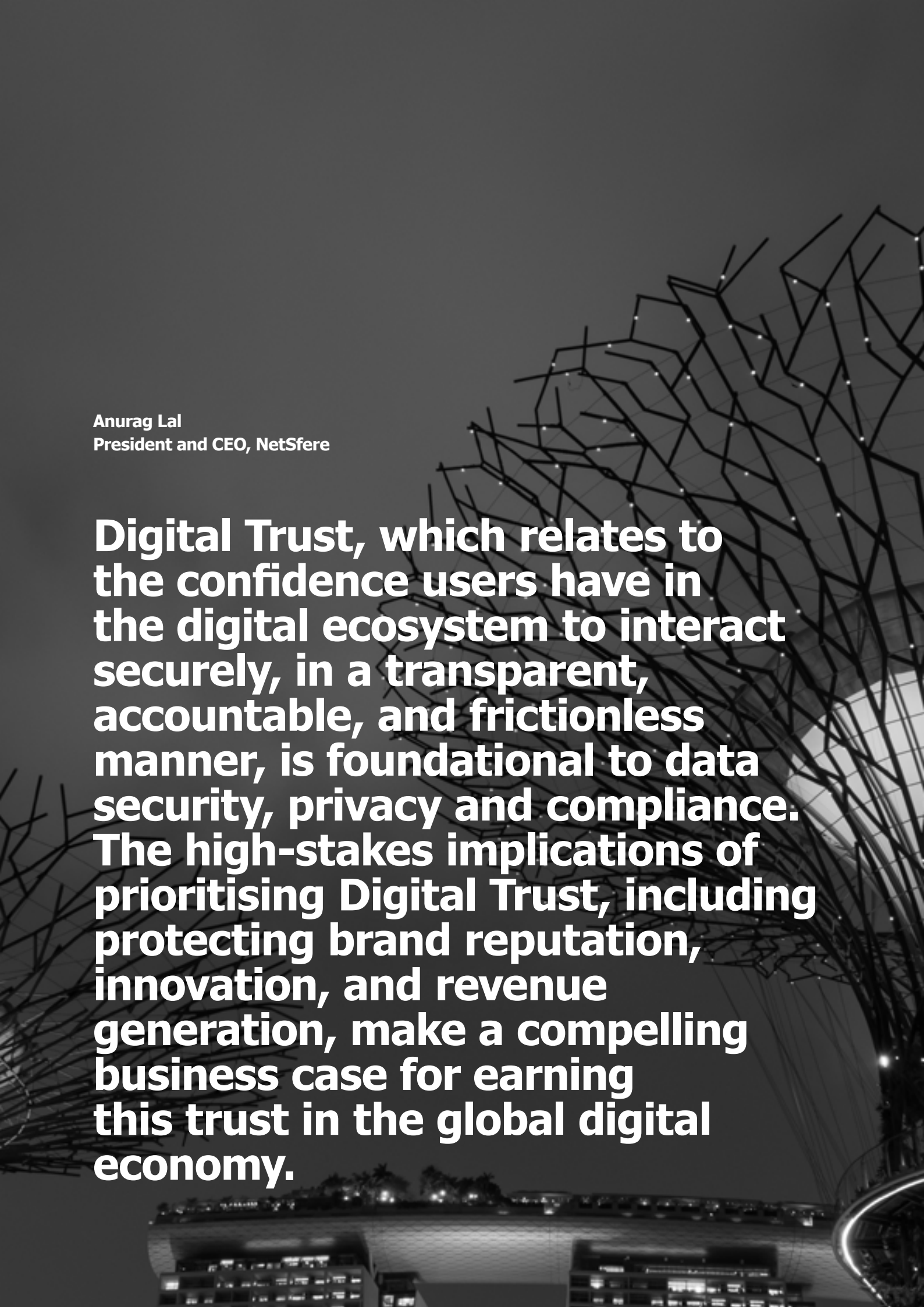
The push to digitalise and innovate has opened a can of challenges for companies, who must consider new privacy, security, and information-control issues as they collect and store more data. These concerns are exacerbated by increasingly polarised views on important topics, the spread of misinformation, and cybercrimes. SGTech believes that building digital and data systems based on trust is key to surmounting these challenges.

Our purpose in commissioning this study is to provide a global orientation of Digital Trust, its opportunities and challenges, and Singapore's importance as a global node for data and digital innovation. Digitalisation offers new approaches to trust. Competitors who do not see eye-to-eye can still transact efficiently because technologies such as privacy-enhancing technologies and distributed ledgers (also called shared ledgers), coupled with good governance in processes now enable these interactions even without parties knowing who they transact with.

Our study identified governance, technology, and people as three pillars that hold up the Digital Trust framework. Each pillar has enablers crucial to building a robust and trusted digital ecosystem. Cross-border cooperation, harmonisation of standards, and mutual recognition of certifications must continue to be encouraged. Education and capability-building of people will also be essential.

We hope this paper is helpful as a starting point to frame the subject. Beyond this whitepaper, more resources will be available at SGTech's Digital Trust Centre of Excellence. We invite you on this journey with us as we strengthen trust and further our common human pursuit of progress.

On behalf of SGTech, I would like to thank our members, industry partners, and the many contributors and interviewees who played a part in this Digital Trust Landscape Study. We are also grateful to the paper's presenting sponsors, AWS and NetSfere, as well as our supporting sponsors, Intel, Lenovo, and Microsoft.



Anurag Lal
President and CEO, NetSfere

Digital Trust, which relates to the confidence users have in the digital ecosystem to interact securely, in a transparent, accountable, and frictionless manner, is foundational to data security, privacy and compliance. The high-stakes implications of prioritising Digital Trust, including protecting brand reputation, innovation, and revenue generation, make a compelling business case for earning this trust in the global digital economy.

2 Foreword

Anurag Lal

President and CEO, NetSfere

This paper provides valuable insights and actionable strategies aimed at strengthening Singapore's digitalisation efforts and furthering Singapore's ambition to become a global node for Digital Trust. In the digital-first era, enterprises are increasingly communicating, collaborating, connecting, and transacting across channels. As the adoption of digital technology continues at a rapid pace, Digital Trust is elevated to a critical business enabler.

Digital Trust, which relates to the confidence users have in the digital ecosystem to interact securely, in a transparent, accountable, and frictionless manner, is foundational to data security, privacy and compliance. The high-stakes implications of prioritising Digital Trust, including protecting brand reputation, innovation, and revenue generation, make a compelling business case for earning this trust in the global digital economy.

Recognising the broad economic implications of earning Digital Trust, Singapore continues to invest in technological and skills initiatives to foster the growth of the Digital Trust ecosystem. In the thriving digital hub that is Singapore, opportunities abound for building digital services based on trust. And, as a leader in transparent governance, trusted regulatory frameworks and a respected centre of finance and law, Singapore is well-positioned to solidify its status as a leader in Digital Trust.

A key to establishing and advancing Digital Trust leadership involves working with security-first, privacy-first business partners that meet the operational imperative of earning and maintaining Digital Trust. This is especially critical in today's hybrid and remote working environments where more business than ever is conducted across digital channels.

A first line of defence for protecting Digital Trust is secure communication and collaboration technology, with end-to-end encryption and robust IT administrative controls. Enterprise-grade technology like this is a major strategic imperative for building Digital Trust, that ensures business continuity in a secure and compliant hybrid and remote working environment.

At NetSfere, we are partnering with Singapore-based companies in a wide range of sectors including financial services, healthcare, and government, to build a more trusted digital ecosystem and contribute to positioning Singapore as a global node for digital and data, built on trust.

We thank SGTech for commissioning this important report which maps out a strategic roadmap for developing Digital Trust in Singapore; all of the many contributors from around the world for providing their valued insights; and Eden Strategy Institute for compiling the insights and data into this whitepaper.

3 Executive Summary

Digital Trust is a SGD 385 bn (USD 270 bn) global market opportunity and is expected to grow to SGD 765 bn (USD 537 bn) by 2027. Digital Trust will also enable further growth in other sectors in the digital economy.

Trust has been a competitive edge for Singapore and led to its early success as a regional hub and attractive home for global businesses. An increasingly digital world amplifies opportunities for Singapore beyond the region, but only if Singapore can continue to be a trusted partner. With this lens, SGTech commissioned Eden Strategy Institute to study the Digital Trust landscape to help frame the topic and highlight the challenges and opportunities. This paper is a succinct summary of the broader landscape study conducted.

Between January and August 2022, an exhaustive review of existing Digital Trust literature and a series of over 80 interviews were conducted worldwide with leading experts in various Digital Trust domains. Through these insights, and extensive deliberations with SGTech's Digital Trust Committee and Council members, we have defined Digital Trust as follows:

> **Digital Trust is the confidence participants have in the digital ecosystem to interact securely, in a transparent, accountable, and frictionless manner.**

To achieve this, a range of enablers in Governance, People and Technology has been identified:

- **Governance:** Facilitate greater digital participation among good actors in an ethical manner, while putting in place mechanisms that resolve conflicts
  - AI Ethics Frameworks
  - Data Protection Laws and Regulations
  - Cyber Strategy and Laws
  - Cyber Insurance
  - Privacy by Design
  - Security by Design
  - Harmonisation Of Standards
  - Facilitating Bodies and Associations
  - Recourse and Mediation Bodies

- **People:** Develop discerning digital natives who can navigate the proper use of data and information, while keeping themselves and the organisations safe from bad actors
  - Consumer Awareness and Education
  - Citizen Advocacy
  - Digital Trust Certifications
  - Digital Trust Workforce
  - Digital Trust-Related Consultancy: Legal, Resilience Building, Training, Cybersecurity As-A-Service, Privacy-As-A-Service

- **Technology:** Overcome legal barriers while keeping in place the spirit of those laws, enhance online safety, and keep secure data and digital transactions from bad actors
  - Privacy Enhancing Technologies
  - Distributed Ledger Technologies
  - Cybersecurity Technologies
  - Digital Identity
  - Governance, Risk, and Compliance Software
  - AI/ML Tools: e.g., Fraud Detection, Threat Monitoring

Five key trends and opportunities were also identified in this study:

#1 Misinformation is becoming more widespread and affecting everyday people

- Consumer awareness and education to enable a more discerning population is essential

#2 Expectations on privacy and responsible use of data have grown and become mainstream

- The use of Privacy Enhancing Technologies (PET) could help adhere to the letter and spirit of the law, while generating the benefits that come from data sharing and analysis
- Embedding Privacy in products and services through Privacy by Design enhances transparency and accountability in an organisation's systems, and helps to increase confidence and loyalty in consumers and businesses they transact with

#3 Cybercrimes continue to grow unabated, especially in the Asia-Pacific

- Large companies will need to build up resilience capabilities, while Small and Medium Enterprises (SMEs), that are generally under-resourced, should consider cyber-as-a-service offerings
- Both large companies and SMEs should consider cyber insurance

#4 Data localisation, sovereignty and cross-border data flow issues are high on the agenda for many countries

- There is a strong need for data-sharing standards to be harmonised across countries, and there are opportunities to mutually recognise certificates that relate to Digital Trust; facilitation bodies such as APEC Business Advisory Council (ABAC) are important players that can drive these efforts
- Adoption of technologies, such as Digital Identity and permission-based Distributed Ledger Technologies, can also assist with more seamless and efficient cross-border interactions

#5 Growing demand for Digital Trust skills and risk management solutions

- A more sophisticated Digital Trust workforce will need new skills, as well as related services such as consultants, lawyers, training providers, and certification agencies
- Software solutions in Governance, Risk and Compliance (GRC) can also help companies better manage organisational risk and requirements for continuous compliance

There is no magic bullet to Digital Trust. Like trust in the physical world, Digital Trust takes time and effort to build up. The promise of Digital Trust is not just in the SGD 765 bn (USD 537 bn) industry that will be realised in 2027, it is the broader enablement of the digital economy and surmounting the trust challenges of today. These will result in a manifold multiplier in terms of more digital transactions and less losses from issues such as cybercrime. It offers new opportunities and a true differentiation to countries and companies that embrace it. We hope this paper helps you think more holistically about Digital Trust and provides pointers on where to start.

4 Introduction

Fostering trust in the digital world is increasingly vital in today's age of industry digitalisation, misinformation, and changing societal attitudes towards privacy.

There are many facets to the megatrend of Digital Trust. Digital Trust encompasses more than cybersecurity, privacy, data protection, or Artificial Intelligence (AI) ethics. At its core, creating Digital Trust demands no less than a concerted, full set of approaches that uphold stakeholder confidence and ensure that digital interactions truly work.

This paper aims to:

- Offer a broader definition of Digital Trust;
- Provide a global orientation on trust-related challenges in the digital arena;
- Provide a glimpse into the opportunities in Digital Trust; and
- Highlight Singapore's importance as a global digital and data node, built on trust.

Trust has always been foundational to Singapore's early success as a facilitator and partner for regional networks and global companies. A digital world opens Singapore up to wider global networks and opportunities. Its people, processes, and governance structures must be ready for the corresponding challenges, and Digital Trust is core to this readiness.

Singapore has been amongst the most progressive countries in Digital Trust:

- Recently opening a Digital Trust Centre focusing on trust technologies[1];
- Developing a Model AI Governance Framework and AI Body of Knowledge[2];
- Passing the Protection from Online Falsehoods and Manipulation Act (POFMA) in 2019[3];
- Implementing the Personal Data Protection Act (PDPA) in 2012, and rolling out Data Protection Officers (DPO) across its companies[4];
- Enabling Singpass, its national Digital Identity system, to be ubiquitous across government e-services and covering over 97 percent of eligible residents[5]; and
- Developing various Data Sharing Frameworks by the Infocom Media Development Authority (IMDA), Monetary Authority of Singapore (MAS)/Association of Banks in Singapore (ABS), and Singapore's Smart Nation and Digital Goverment Office (SNDGO)[6].

But more can always be done to unpack and frame the issues around the topic. This paper is the synthesis of a landscape study undertaken by the Digital Trust Committee of SGTech, Singapore's leading trade association for the tech industry, between January and August 2022. Eden Strategy Institute performed an exhaustive review of the global literature on Digital Trust and conducted a series of over 80 interviews across the world with leading experts in various Digital Trust domains.

5 What is Digital Trust?

From our expert interviews, review of existing Digital Trust literature[7], and deliberations with SGTech's Digital Trust Committee and Council members, this paper proposes a broader view of Digital Trust that extends beyond security.

Much of the existing Digital Trust literature has focused on cybersecurity and the components that secure digital systems and data flows. With legislative developments such as General Data Protection Regulation (GDPR) in Europe or PDPA in Singapore, the awareness of user privacy has been building up. In a trusted environment, there are opportunities to make digital transactions easier for everyone, allowing for individuals, businesses, and government participants to interact effortlessly across borders.

This paper therefore proposes the following definition of Digital Trust:

> **Digital Trust is the confidence participants have in the digital ecosystem to interact securely, in a transparent, accountable, and frictionless manner.**

This broad definition further finesses different emphases of Digital Trust for various stakeholders.

Citizens

Digital Trust is the confidence citizens have when they are interacting online, that their interactions are secure, remain private, transparent, and accountable.

Industry and Businesses

A business can inspire Digital Trust by being secure, competent, consistent, and transparent, and having a verifiable commitment to user interests, as demonstrated by its policies, systems, and conduct.

Governments and Regulators

Digital Trust is the adherence to necessary processes, policies, and frameworks around security, transparency, and accountability by the Government to enable businesses and consumers to interact efficiently and confidently in the digital world.

6 Challenges

To strengthen Digital Trust, it is useful to understand the challenges that will need to be addressed for the different stakeholders. There are a plethora of challenges but we present the most important challenges across our interviews.

Citizens

Misinformation

- Misinformation
- Disinformation
- Deepfakes driven by bad bots and foreign actors seeking to influence society

Online scams

Including:

- Hacking scams
- Phishing scams

Misuse of data

Where data analysis and personal information is used without consent

Online harms

Beyond misinformation, other forms of online harms such as:

- Child sexual exploitation and abuse content
- Cyberbullying
- Hate speech
- Online addiction
- Terrorism-related content
- Violent content

Misleading user interfaces

Where dark patterns and corporate interests misdirect consumers in their online interactions

Industry and Businesses

Constant cyber threats

Ensuring data and transmission are secure from external and internal intrusions, with necessary redundancy to recover from breaches

Navigating complex regulations

Adhering to local and global regulations which are often disjointed and require local customisation; potentially high financial penalties for privacy regulatory failures

Inadequate capabilities

- Lack of baseline internal staff capability
- Hiring for specific skills such as cybersecurity and privacy engineers
- Retaining external support such as Digital Trust lawyers and Cybersecurity consultants

Lacking standards related to Digital Trust

Lack of standards that go beyond IT and cybersecurity, such as AI ethics frameworks, data sharing policies, or data classification

Constraints in data sharing

- Lack of trust between counterparties
- Data sovereignty and national laws restrictions
- Lack of available technology to manage Personal Identifiable Information (PII)

Under-resourced SMEs

Small and Medium Enterprises (SMEs) are especially vulnerable to cyber attacks, due to their lack of financial and manpower resources to put in place the necessary safeguards

Governments and Regulators

Facilitating data flows

Facilitating data flows, business cooperation within the country and across borders, while maintaining privacy concerns, cybersecurity, and national security

Complexities in cross-border cooperation

- Ensuring cross-border cybersecurity enforcement and sharing of intelligence on threats
- Cross-border data standards harmonisation through working with other governments and standard bodies

Foreign interference and disinformation

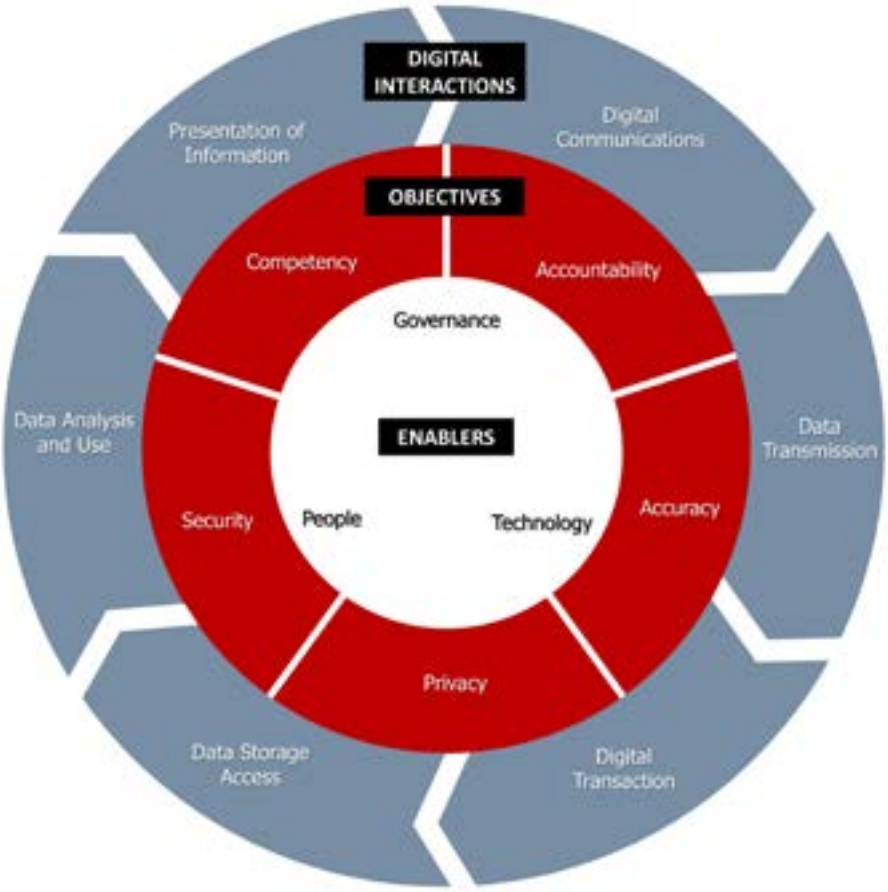
Educating the population and putting up defences to counter online threats

Global competition for talent

The global pull of Digital Trust-related talent such as in:

- AI ethicists
- Cybersecurity
- Digital Identity specialists
- Lawyers trained in international privacy regulations
- Privacy engineers

7 Enabling Digital Trust



Countries and organisations have a variety of options to holistically enable more trusted Digital Interactions.

There are five primary forms of Digital Interactions.

- **Presentation of Information:** e.g., Website viewing; hardware interfaces
- **Digital Communications:** e.g., Chats; video conferencing
- **Data Transmission and Digital Transaction:** e.g., IoT device transmissions; eCommerce transactions; B2B data transactions
- **Data Access and Storage:** e.g., Cloud storage; APIs; Digital IDs
- **Data Analysis and Use:** e.g., AI and Big Data analysis; wearables health monitoring; Know Your Customer (KYC)

The key objectives of Digital Trust in these interactions are:

- **Accuracy:** Information and data sources are accurate, timely, and comprehensive
- **Privacy:** Legal compliance and user confidentiality is respected
- **Security:** Data and transaction integrity is maintained and available only to the intended parties
- **Competency:** Digital Interactions are available and done efficiently and successfully
- **Accountability:** Use of the data or purpose of the use meets expectations and is done in a legal, ethical, and transparent way; failures such as data breaches or misuse of data are addressed quickly and responsibly

To enable these objectives, three sets of Enablers in Governance, Technology, and People are required:

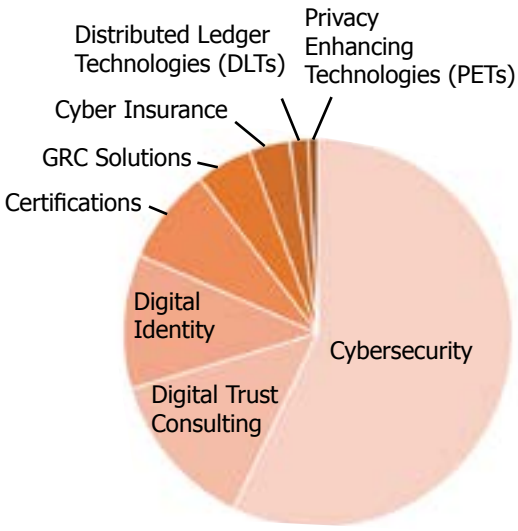
- **Governance:** Facilitate greater digital participation among good actors in an ethical manner while putting in place mechanisms that resolve conflicts
  - AI Ethics Frameworks
  - Data Protection Laws and Regulations
  - Cyber Strategy and Laws
  - Cyber Insurance
  - Privacy by Design
  - Security by Design
  - Harmonisation Of Standards
  - Facilitating Bodies and Associations
  - Recourse And Mediation Bodies

- **People:** Develop discerning digital natives who can navigate the proper use of data and information, while keeping themselves and the organisations safe from bad actors
  - Consumer Awareness and Education
  - Citizen Advocacy
  - Digital Trust Certifications
  - Digital Trust Workforce
  - Digital Trust-Related Consultancy: Legal, Resilience Building, Training, Cybersecurity As-A-Service, Privacy-As-A-Service

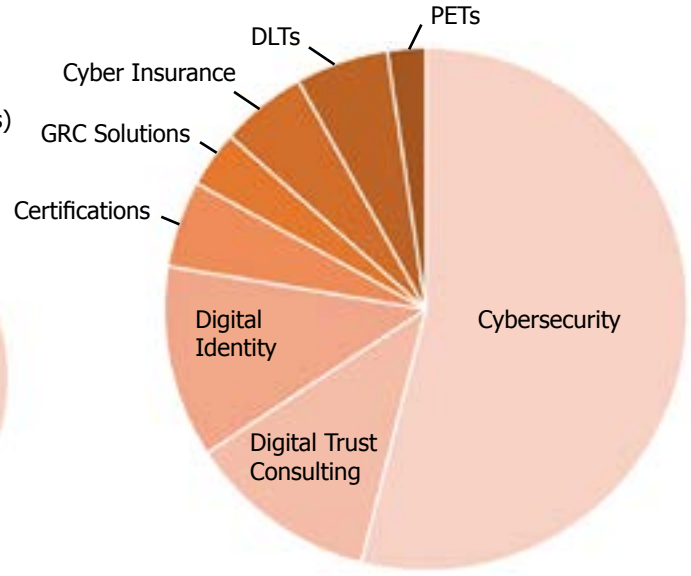
- **Technology:** Overcome legal barriers while keeping in place the spirit of those laws, enhance online safety, and keep secure data and digital transactions from bad actors
  - Privacy Enhancing Technologies
  - Distributed Ledger Technologies
  - Cybersecurity Technologies
  - Digital Identity
  - Governance, Risk, and Compliance Software
  - AI/ML Tools: Fraud Detection, Threat Monitoring, Synthetic Data, etc.

8 Sizing the Market for Digital Trust

Digital Trust presents a global market opportunity of SGD 385 bn (USD 270 bn) currently and is expected to grow to SGD 765 bn (USD 537 bn) by 2027.



Global Revenues by Digital Trust Enabler (SGD bn; 2022)



Global Revenues by Digital Trust Enabler (SGD bn; 2027 Estimates)

	Headline	SGD bn 2022	2027	CAGR
	Cybersecurity	220	413	13%
	Digital Trust Consulting	51	90	12%
	Digital Identity	43	91	16%
	Certifications	31	41	6%
	GRC Solutions	18	27	9%
	Cyber Insurance	13	41	25%
	Distributed Ledger Technologies (DLTs)	6	44	49%
	Privacy Enhancing Technologies (PETs)	3	18	40%
	Industry Total	**385**	**765**	**15%**

Source: Eden Strategy Institute Interviews and Analysis; Globe Newswire; Statista; Fortune Business Insights; Consultancy.org, IDC; Report Linker

Based on our research, interviews, and analysis, the global market for Digital Trust is growing at a Compounded Annual Growth Rate (CAGR) of 15 percent, and is expected to double to SGD 765 bn (USD 537 bn) over the next five years.

The size of the Digital Trust sector in Singapore currently stands at SGD 1.7 bn (USD 1.2 bn) (yearly revenue) with more than half of this coming from Cybersecurity. The sector also currently employs around 15,000 people and could grow to SGD 4.8 bn (USD 3.4 bn) (yearly revenue) and employ 34,000 to 45,000 people by 2027.

Cybersecurity, the most mature and largest segment, will continue to contribute most significantly in absolute terms. Digital Identity is also a relatively mature technology, with adoption continuing to pick up, as more countries look towards national digital transformation plans. For example, India has shown admirable success in creating the world's largest biometric Digital ID system, with its Aadhaar program enrolling 1.3 bn citizens (or 99 percent of Indian adults)[8]. The European Commission proposed a digital ID scheme in 2021, that could be used across the EU by more than 80 percent of the EU population by 2030[9]. China's Prime Minister Li Keqiang has recently announced that Digital IDs, which have been tested in China since 2018, will be rolled out nationwide in 2022[10]. Cross-border economic opportunities are also expected to be amplified, should these national Digital IDs become harmonised or interoperable regionally.

The market for emerging Digital Trust Technologies such as Privacy Enhancing Technologies (PETs) and Distributed Ledger Technologies (DLTs) is attracting venture capital interest, and companies are working to validate use cases for different types of data in various industries. Their potential to leapfrog regulatory requirements and scale trust in their systems makes them exciting hotspots for growth.

Cyber Insurance is gaining greater adoption from large companies, and is also expected to see an uptick from more widespread SME adoption.

Insurance companies are actively courting SMEs to help diversify their own risk portfolios.

Consulting, Certifications, and GRC Solution providers are capability-building sectors that tend to be early adopters, which will help accelerate Digital Capabilities across different industries and improve risk management practices.

SGD 765 bn

Global market for Digital Trust in 2027 (USD 537 bn), doubling from SGD 385 bn (USD 270 bn) in 2022

SGD 4.8 bn

Size of Singapore's Digital Trust Sector in 2027

34 - 45k

Size of Singapore's Digital Trust workforce in 2027

9 Global Trends and Opportunities in Digital Trust

Distrust is now society's default emotion, with six in ten people inclining to distrust until they see evidence to suggest that something is trustworthy.[11]

Seven percent more people in 2022, compared to 2021, believe that business leaders are purposely trying to mislead through false or exaggerated information. Mistrust towards media and government leaders is also proliferating, growing at a higher rate of eight and nine percent respectively.[12]

Covid-19 has accelerated digitalisation and teleworking, but it has also brought several challenges to the fore. Trust in technology companies in 2021 dipped to an all-time low, as the world grappled with increased cyber-attacks, data breaches, and 'bad bots' driving misinformation. Governments were not spared either; for example, democracies such as Australia, Germany, the Netherlands, South Korea, and the US saw the greatest declines in trust in 2022.[13]

Now, more than ever, governments and companies need to pay attention to Digital Trust. Based on our research and interviews with experts from domains of Digital Trust, the following five issues present the greatest challenges in Digital Trust to countries and organisations and need to be addressed.

#1 Misinformation is becoming more widespread and affecting everyday people

Fake news and misinformation driven by bots; fake unauthenticated accounts; "online trolls"; and foreign nation-state actors, are all eroding Digital Trust among consumers and citizens globally. It is becoming increasingly complex to distinguish between semi-true information and complete misinformation, and technology has not developed enough nuance to tackle this issue in a scalable and consistent way.

Singapore is ranked second among countries whose Internet traffic has high bad bot activity, according to a study across 192 countries. 39 percent of Internet traffic in Singapore was from bad bots, used to conduct malicious attacks, compared to 53 percent from people and eight percent from good bots.[14]

In a global survey across 25 economies, 86 percent of online respondents globally believe they have been exposed to fake news. Of these, over 85 percent reported that they initially believed it[15]. Although in Singapore most citizens do not deliberately spread fake news, they are exposed to misinformation by accessing global social media platforms and as many as 75 percent have unwittingly forwarded such information onto their personal networks.[16]

86%

Proportion of online respondents that believe they have been exposed to fake news[17]

39%

Bad bots as a proportion of Internet traffic in Singapore[18]

OPPORTUNITIES

Consumer Awareness and Education

More governments will act defensively and enact laws related to misinformation. For example, Singapore has passed the Protection from Online Falsehoods and Manipulation Act (POFMA), which seeks to counteract false or misleading information online[19]. This law covers public as well as closed platforms such as chat groups and social media groups.

Our interviews have indicated that social media companies are presently concerned about this issue, are taking decisive actions themselves, such as hiring large global teams to police content, deploying AI-based technologies to identify fake accounts, and limiting the spread of misinformation.

Governmental oversight and social media self-policing is necessary but not sufficient. There is a need to develop a more discerning population. **Greater consumer awareness and education** will be vital to manage the spread of misinformation, which presents an opportunity for governments, educational institutions, think-tanks, non-profits, and advocacy groups. School curricula and community awareness programs, particularly for the elderly, will also be necessary to improve consumer online savvy.

#2 Expectations on privacy and responsible use of data have grown and become mainstream

There has been a renewed demand for privacy, as a result of the missteps of social media giants and misuse of Big Data, such as in the Cambridge Analytica data scandal where personal data of users was collected and used without consent for targeted political advertising[20]. The growing awareness of data bias and opaque decision-making in AI, which in some high-profile cases has resulted in racial profiling[21], has also prompted caution and unease in the use of AI.

Globally, 80 percent of countries have some sort of data privacy regulation or draft data privacy regulation[22]. Europe has traditionally been the dominant force in privacy regulation with the EU General Data Protection Regulation (GDPR), for which Germany and France are key anchor nations[23]. The proliferation of data regulations has accelerated, with Asia, Africa, and South America coming on board with their own data protection laws.

However, this number is only 69 percent for Asia-Pacific Countries[23]. More developed privacy regime standards are expected to take form, with more countries following the stringent standards found in EU GDPR, such as provisions on extra-territorial reach and data transfer.

Many ASEAN countries have based their privacy regulations on the GDPR, although privacy regulations are at different stages of development. Many governments in the region are still educating themselves on data privacy approaches that would be appropriate to their contexts, and have yet to institutionalise new regulations.

Chinese tech companies are ramping up their privacy protections to meet the expectations of the national government and Chinese people, to be more transparent, secure, and accountable, as well as to fully comply with the recently passed Personal Information Protection Law (PIPL)[24].

The US does not have a comprehensive federal level data privacy law, although one is currently being negotiated. Nonetheless, there is a growing number of states that have adopted their own data protection laws, such as the California Consumer Privacy Act (CCPA) which came into effect in January 2020, and the California Privacy Rights Act (CPRA) which comes into effect in January 2023[25].

Singapore has an AI framework to guide companies on ethical AI use[26], without legislating specific AI laws so far. Countries such as the UK, US, and Spain passed AI-related legislation in 2021. The EU is now working on an EU AI Act, which could influence other countries' AI standards, akin to how the EU GDPR has influenced many countries' privacy policies. More than 60 countries have adopted some form of AI policy[27], as the world ramps up the pace of AI adoption.

69%

Proportion of Asia-Pacific Countries that have data privacy regulation or draft data privacy regulation[28]

OPPORTUNITIES

- **Privacy Enhancing Technologies (PETs)**
- **Privacy by Design**

Increasing privacy governance requirements are at odds with the increasing ways data is used, such as with Artificial Intelligence / Machine Learning (AI/ ML) models. **PETs** are a collection of methods to do encrypted computation on sensitive or protected data, such as Personal Identifiable Information. PETs can satisfy data-sharing constraints imposed by privacy regulations.

They can also help hide sensitive non-private data, such as telco tower geolocations, fleet routes, or eCommerce buying patterns. These technologies promise a future where datasets will no longer need to be exchanged, for cross-dataset machine learning benefits to be reaped.

PETs will unlock more AI/ML use cases and advance new insights. We see a future where datasets are made voluntarily available across different industries; there are already green shoots of consortiums such the Melloddy Project – a group of pharmaceutical companies including GSK, Bayer, and Merck – collaborating on drug discovery because richer datasets have been made available. Regulations around AI use will be even more critical in this supercharged environment. Countries and companies will need to have in place their own AI frameworks as well as governance policies.

But privacy regulations and PETs are only part of the solution. The default posture of companies should be to provide privacy assurance across their products and services, embedded into the design and architecture of IT and business practices.

Interviewees reported increases in revenue and customer loyalty, with consumers feeling safer and more confident to interact with companies that they feel are accountable and transparent in how they use their data. To achieve this, organisations can consider adopting the principles of the **Privacy by Design** Framework, developed by former Ontario Privacy Commissioner Ann Cavoukain, which outlines seven foundational principles[29].

#3 Cybercrimes continue to grow unabated, especially in the Asia-Pacific

There has been a rise in cyber-related crime globally. Worldwide cybercrime cost USD 6 trn in 2021, growing at 15 percent Y-o-Y reaching USD 10.5 trillion by 2025[30]. Ransomware is the fastest-growing cybercrime, with damages in 2021 estimated at USD 20 bn - 57 times more than it was in 2015[31]. Ransomware repercussions can be significant. In May 2021, the Colonial Pipeline fuel company in the US was forced to pay USD 5 mn in ransom, and the attack caused major gas shortages in the southeast coast of the US[32].

The growth in cyberattacks in Asia-Pacific is perhaps more serious than the global average, with a 168 percent increase between May 2020 and May 2021 alone[33]. Dark net-related arrests in Southeast Asia have increased in recent years, indicating that criminals perceive the region as a low-risk/high-gain operational environment, where the likelihood of detection remains relatively low.

The region is plagued with enforcement and coordination problems. Regional threat assessment sharing and mapping of cybercrime are missing. Crimes are often cross-border, making enforcement difficult. Penalties also do not seem proportionate to the harm done, and cyber criminals around the region understand how to work the system to reduce their culpability.

Regional players see Singapore as serious about cybersecurity. Singapore has a dedicated Cybersecurity Act, a clear Cybersecurity Strategy developed in 2021, and a vibrant cybersecurity ecosystem underpinned by a strong Cybersecurity Agency. Nonetheless, it is a target as it has a big financial sector, and is one of the most connected nations in the world. Singapore is constantly under threat, with cybercrime comprising 48 percent of all crime in the country.[34]

Cybercrime Statistics

Global	US	Asia-Pacific	Singapore
USD 6 trn	**300%**	**168%**	**38%**
Cost of Cybercrimes in 2021[35]	Increase in Cybercrimes reported by the FBI since the pandemic[36]	Increase in Cyberattacks between May 2020 and May 2021[37]	Growth of Cybercrime cases between 2020 and 2021[38]

OPPORTUNITIES

- **Resilience Building in Large Enterprises**
- **Cybersecurity as-a-Service for SMEs**
- **Cyber Insurance**

Large enterprises and governments will constantly play a game of cat and mouse with cyber criminals. Cybersecurity products also tend to be costly and catered more towards large enterprises. Beyond shoring up on products and talent, sophisticated **large enterprises will build up resilience capabilities** and be able to respond and recover from cyber-attacks. Large companies should line up their public relations, legal, and forensic consultants before an incident happens, as there is little time to react by the time a breach occurs.

Governments and large enterprises can look at roadmaps and frameworks such as Singapore's Cyber Security Agency Cyber Trust Certification's Five Tiers[39] to understand how they can advance in the journey.

Most vulnerable are SMEs who lack resources and awareness about improving cyber hygiene. Many small companies are at a loss on where to start. SMEs are unlikely to add headcount for cybersecurity and should consider **Cybersecurity as-a-Service** (ie. outsource their cybersecurity needs) from third-party companies. However, these services will have to be priced low to serve this price-sensitive market, and even subsidised by the government as a public good.

Cyber Insurance is an interesting area which can spur cyber hygiene, as getting it requires companies to adopt a certain standard of corporate cyber-readiness. We estimate the demand for Cyber Insurance to be growing at 25 percent Y-o-Y. There is an increased interest from insurance companies to expand their offerings to SMEs to diversify their portfolios. By using Cyber Insurance, companies can protect against losses stemming from data destruction, theft, extortion, hacking, and network intrusion or interruption. Increased awareness and adoption of Cyber Insurance should be considered by all large companies and even most SMEs.

25%

Annual Cyber Insurance market growth

#4 Data localisation, sovereignty, and cross-border data flow issues are high on the agenda for many nations

62

Countries that have enacted data localisation requirements[40]

The importance of localisation and sovereignty has risen over the years due to privacy concerns, cybersecurity, and national security. More than 62 countries have enacted data localisation requirements in 2021, up from 35 in 2017. The number of related policies has also doubled from 67 to 144 in the same period[41]. For example, China requires data localisation for the broadly-defined Critical Information Infrastructure operators. Transferring data outside of China involves security assessments conducted by the Cyberspace Administration of China (CAC)[42].

Pivotal events such as the Edward Snowden National Security Agency (NSA) data collection revelations[43], as well as the enactment of the US Patriot Act[44] - which allows the US government to access information from US-based servers - have further heightened national data sovereignty concerns around the world. Nonetheless, the US is one of the strongest opponents to data localisation restrictions; there are no special requirements to transfer personal data from the US to third-party countries.

The EU is more restrictive but does not require certain personal information to remain in the EU. Cross-border data transfers to third-party countries, however do need to respect GDPR either through being countries on the EU "Adequacy Decision" list, or applying appropriate safeguards such as Standard Contractual Clauses (SCCs). It should be noted that only 14 countries are on the Adequacy Decision list, with no ASEAN representation. 94 percent of global data transfers are based on Standard Contractual Clauses[45].

These policies make cross-border data flows difficult. Complying with cross-border data transfer laws is cited as the most difficult task for privacy professionals[46].

To address this, ASEAN is trying to move together on data protection and data flows. For example, ASEAN has already implemented Model Contract Clauses for cross-border data flows[47]. These are important steps in coordinating data regulatory policies. Strategic priorities for the ASEAN Digital Data Governance Framework include data flow mechanisms with particular focus on certification as well as regulatory sandboxes. The Philippines and Singapore are like-minded partners driving this trend, and are instrumental in the adoption of the ASEAN Digital Data Governance Framework.

OPPORTUNITIES

- **Harmonisation of Standards**
- **Facilitating Bodies and Associations**
- **Digital Trust Certifications**
- **Cross-border Digital Identity**
- **Permission-based Distributed Ledger Technologies (DLTs)**

Associations and harmonised standards will play increasingly important roles to facilitate data sharing. Various initiatives such as the APEC Cross-border Privacy Rules (CBPR) and Global CBPR Forum seeks to help companies share data through common standards and mutual recognition of certificates[48]. SGTech and the APEC Business Advisory Council (ABAC) have entered into a partnership to further the APEC CBPR agenda as well as develop a Digital Trust Centre of Excellence to promote greater multi-lateral trust mark integration and recognition. These efforts will take time to develop momentum, and will benefit from greater participation among both countries and companies globally.

As more countries create Digital Trust-related policies, more companies will adopt various **Digital Trust certifications** as a source of validation and prove their trustworthiness. APEC CBPR is one such certification for data sharing, and others include the ISO 27001 on information security, CSA Cyber Essentials and Cyber Trust marks for cybersecurity, and GDPR and PDPA practitioner certifications for personal data protection that touch on the other aspects of Digital Trust.

Trust-related technologies such as **Digital Identity, Distributed Ledger Technologies (DLTs)**, and PETs can also help play a role in improving data flows. Digital Identity helps verify the authenticity of information, be it from a company, individual, or IoT device. Opportunities for cross-border collaboration on Digital Identity will help to reduce frictions in data flow and data access, and could even spur greater cross-border digital transactions. Companies such as Mastercard[49] are seeking to help orchestrate these cross-border Digital Identity collaborations, developing technology, liability, assurance, and commercial frameworks to enable this.

The resilience, transparency, and accountability found in DLTs has garnered strong interest from regulated industries, especially within the financial services sector, through "Private" blockchains where participants are validated before being accepted. The Monetary Authority of Singapore (MAS) has undertaken a series of experiments looking at several use cases for DLTs, such as tokenisation of the SGD, local and cross-border inter-bank payments and settlements, and Central Bank Digital Currency (CBDC). It actively involves the private sector and other central banks in these collaborations. For example, its most recent initiative, Project Dunbar[50], is a collaboration between MAS, the BIS Innovation Hub Singapore Centre, the Reserve Bank of Australia, Bank Negara Malaysia, and the South African Reserve Bank.

Even though ASEAN countries are still in the early phase of DLT adoption, blockchains already feature in all ASEAN Member's ICT Master Plans[51]. DLT's consensus mechanisms enable data and its processing to be resilient from attacks, allowing control to be held in the hands of the registered participants themselves. There is no need to either trust the counterparty or rely on an intermediary to process, as the transaction is verified by the system's specified governance protocol.

#5 Growing demand for Digital Trust skills and risk management solutions

Government regulations and data protection fines are on boardroom agendas, as they now pose existential risks for companies. In Singapore, the maximum financial penalty that may be imposed on organisations for PDPA breaches has now increased from the previous maximum of SGD 1 mn, to SGD 1 mn or 10 percent of the organisation's annual turnover, whichever is higher[52]. Similarly, companies with EU exposure can be fined up to EUR 20 mn or four percent of worldwide turnover (whichever is greater) for GDPR breaches[53].

This has created a demand for new specialised Digital Trust skills such as privacy engineers and Data Protection Officers (DPO). These roles are increasingly important to large organisations that deal with large amounts of data, such as large consumer tech companies. Small companies in Singapore are also required to designate at least one individual to act as a DPO. There is also a war on talent for "traditional" cybersecurity professionals. The number of unfilled cybersecurity positions globally is growing from one million in 2013, to an estimated 3.5 million in 2025[54].

Large companies are also beginning to invest in general Digital Trust education for their employees. These begin with cybersecurity hygiene matters, and can often extend to organisation risk management.

3.5 mn

Estimated number of unfilled cybersecurity positions in 2025[54]

OPPORTUNITIES

- **Digital Trust workforce and skills**
- **Digital Trust Service providers**
- **Adoption of GRC technologies by companies**

A more sophisticated **Digital Trust workforce** and providers of **Digital Trust-related services**, such as consultants, lawyers, and training providers are becoming more prevalent. Digital Trust practitioners will graduate with Degree and Diploma courses in highly-specialised domains. Cutting-edge companies are also looking for multi-disciplinary talent who can bridge the divide between policy, compliance, AI ethics, and technology. In the future, more global companies will form small multi-disciplinary teams with a global Digital Trust mandate, creating strong competition for such talent globally.

Organisations will also look to imbue their entire workforce with Digital Trust-related training. Companies will increasingly invest in continuous compliance and real-time risk assessment. More and more organisations will opt for **Governance, Risk, and Compliance (GRC)** solutions to help them manage this undertaking, where inputs from everyday employees will flow into GRC systems to provide a more macro view of organisational risk. GRC software is already seeing a 20-30 percent increase in interest in Singapore[55] and an eight to 14 percent growth rate globally[56].

10 Concluding Remarks

Royce Wee
SGTech Digital Trust
Exco member &
Lead for Digital Trust
Landscape Study

Digitalisation is one of the key trends of our times. For digitalisation to fulfil its promise, we need to put Digital Trust front and centre of our efforts to develop and regulate the digital economy.

The Digital Trust Landscape Study, as summarised in this paper, represents an essential effort by SGTech and the tech industry to understand and unpack this large, complex, cross-border, and multi-faceted topic through research, interviews, and analysis with experts, government leaders, and captains of industry from around the world.

Having put a solid conceptual framework on what Digital Trust is, its enablers, and its challenges, the Digital Trust Landscape Study is very much at the beginning of its important work.

This is because the study, perhaps more crucially, also represents a clarion call to action for all the essential stakeholders in the digital ecosystem.

First, our laws, policies, and regulations have to be appropriate, balanced, and fit-for-purpose to secure and facilitate Digital Trust. This will ensure that digital technologies continue to be at the service of humans, and enable tech development to be on a healthy and sustainable track.

Second, corporations will do well in viewing the incorporation and demonstration of Digital Trust as a key competitive differentiator and advantage. Where corporations display Privacy by Design and Security by Design, adopt privacy-enhancing technologies and governance, risk and compliance tools, invest in their cybersecurity, and have third-party certifications to review and validate their systems and processes, they are much better-placed to win and retain their customers, as well as innovate using the data they have to come up with new products and services in a responsible and trusted manner.

Third, employees and customers also have much to look forward to. Employees will be able to access new training and upskilling courses to master new Digital Trust capabilities, for instance, across data protection, cybersecurity, fair market conduct, and ethics. Customers will be entitled to greater transparency in the data processing activities of corporations, have more agency and choice over the granting of access to their data, and be able to exercise their data subject rights more easily.

As technology doesn't stand still, there will be a recurring need for Digital Trust to continue to evolve. For example, as Web 3.0 takes shape, marked by greater decentralisation, digital assets, and AR/VR experiences, future research will have to be done across the technology, governance, and people pillars to see how digital trust can take root in and propagate across the Web 3.0 digital ecosystem.

We are on the cusp of great and accelerating change driven by rapid tech changes. By securing Digital Trust through a close and collaborative partnership across the public, private, and people sectors, all of us can have the confidence and optimism to ride the wave of change successfully.

In this regard, SGTech has been having early conversations on Digital Trust which are now becoming regional and global conversations and projects. I urge you to get in touch with SGTech if you would like to learn more, and prepare your organisation to build its capabilities and join our growing Digital Trust ecosystem.

“We are on the cusp of great and accelerating change driven by rapid tech changes. By securing Digital Trust through a close and collaborative partnership across the public, private, and people sectors, all of us can have the confidence and optimism to ride the wave of change successfully.

11 Acknowledgements

The SGTech Digital Trust Committee wishes to acknowledge and thank the numerous contributors who provided their valuable insights that informed this study.

SGTech Digital Trust Committee Patron

Mr Tan Kiat How	Senior Minister of State, Ministry of Communications and Information & Ministry of National Development

SGTech Council Chair

Mr Wong Wai Meng	Chief Executive Officer, Keppel Data Centres

SGTech Council Members

Mr Dutch Ng	Co-Founder & Chief Executive Officer, i-Sprint Innovations
Mr Gavin Chua	Head of Stakeholder Engagement, APAC, Meta Singapore
Mr Ivan Chang Weilong	Consumer Payments, Walt Disney Company
Mr Michael Yap	Co-Founder & Managing Partner, TNB Ventures
Ms Jessie Jie Xia	Global Chief Information Officer, Thoughtworks

SGTech Digital Trust Council

Mr Chun Li	Chief Executive Officer, Lazada Group
Mr Ishan Palit	Member, Board of Management, TÜV SÜD AG
Mr Tham Sai Choy	Independent Board Director, DBS Bank

SGTech Digital Trust Committee Members and Study Advisors

Mr Philip Heah	Chief Executive Officer, Credence Lab & Digital Trust Committee Chairman
Mr Royce Wee	Director, Head of Global Public Policy, Alibaba & Digital Trust Landscape Study Lead
Dr Bhaskar Chakravorti	Dean, Global Business, The Fletcher School, Tufts Univ & Landscape Study Special Advisor
Dr Katharina Von Knop	Founder & CEO, Digital Trust Analytics & Landscape Study Special Advisor
Mr Calvin Chu	Managing Partner, Eden Strategy Institute
Mr Chester Chua	Head of Google Cloud, Government Affairs & Public Policy, Google
Mr David Alfred	Director and Co-Head, Data Protection, Privacy & Cybersecurity Practice, Drew & Napier
Ms Jene Lim	Head of Product Management, Experian Asia Pacific
Mr Raju Chellam	Vice President New Technologies, Fusionex
Mr Satya Ramamurthy	Partner, Head of Infrastructure, Government & Healthcare, Head of Strategy, Advisory, Global Co-Head of Public Transport, KMPG
Ms Sowmya Krishnan	Head of Data & AI, SEA, ThoughtWorks
Ms Thao Dang	Head of Enterprise Modernisation, Platforms and Cloud, ThoughtWorks
Mr William Anstee	Chief Executive Officer, Totally Awesome

Expert Interviewees

Dr Adam Chee	Chief, Smart Health Leadership Centre, Institute of Systems Science, National University of Singapore
Mr Adam Wojtonis	Founder & Chief Executive Officer, MonkPhish
Ms Aileen Chew	Area Country Manager, Mastercard Thailand & Myanmar
Mr Alan Chan	Chief Risk Officer, Lazada Group
Mr Alexandru Caciuloiu	Cybercrime, and Cryptocurrency Programme Coordinator, UN Office on Drugs and Crime (UNODC)
Mr Alister Leong	Vice President - Product, SOL-X
Mr Alvin Toh	Chief Marketing Officer, Straits Interactive
Mr Andre Shori	Chief Information Security Officer for the Asia Pacific Region, Schneider Electric
Dr Andreas Hauser	CEO Digital Service, TÜV SÜD
Mr Ankur Gupta	Senior Vice President – Asia Regional Team, Marsh
Dr Ann Cavoukian	Founder and CEO of Global Privacy and Security by Design
Dr Arianne Jimenez	Privacy and Public Policy Manager, APAC at Meta
Mr Bastian Purrer	Co-founder, HumanID
Mr Bruce Liang	Head of Strategic Projects, SEA Group
Mr Cai Yilun	Head of Presales & Solutions (SEA) SenseTime
Mr Charles Ng	Executive Vice President, Ensign InfoSecurity
Mr Charles Radclyffe	CEO, EthicsGrade
Ms Chatrini Weeratunge	Global Risk Ops, Trust & Safety, Meta
Dr Chi Hung Chi	Director, the Strategic Centre for Research in Privacy-Preserving Technologies and Systems (SCRiPTS), NTU
Mr Chng Kai Fong	2nd Permanent Secretary, Smart Nation and Digital Government Office (Singapore)
Mr Clement Teo	Senior Vice President, Business Assurance (ASEAN) at TÜV SÜD
Mr David Tan	Senior Vice President, Political Risk & Structured Credit ASEAN Sales Leader, Marsh
Mr Deb Pal	Director, Digital Trust/Cyber Security, PwC
Mr Devesh Narayanan	Researcher in AI ethics
Mr Dominic Chan	Director, National Digital Identity, GovTech Singapore
Ms Elizabeth Chee	Head of Govt. & Enterprise Sales, Accredify
Ms Elsie Tan	Country Manager Worldwide Public Sector, Singapore at Amazon Web Services (AWS)
Mr Eoin Fleming	Chief Information Officer, Carnel Group
Mr Henry Quek	Deputy Director (Resilience Cybersecurity Policy & Planning), IMDA
Mr Huang Shaofei	Fellow, Singapore Computer Society Cybersecurity Chapter, Association of Information Security Professionals
Mr Ichiro Seino	Regional Automotive Industry Leader, Marsh Asia
Ms Indra Suppiah	Government Relations Lead – APAC, R3
Ms Jane Lim	Deputy Secretary (Trade), Ministry of Trade and Industry (Singapore)
Mr Jeth Lee	Director of Legal and Government Affairs, Microsoft
Ms Katharine Jarmul	Principal Data Scientist, Thoughtworks
Mr Ken Chua	Group Deputy Director, FinTech Infrastructure Office, FinTech and Innovation Group, MAS
Mr Kenneth Siow	General Manager for Singapore, Malaysia & Indonesia and Regional Director SEA, Tencent Cloud International
Mr Kiat Lim	Privacy Engineer, Google
Dr Konstantinos Komaitis	Independent Policy Consultant and Author
Dr Kuo-yi Lim	Co-Founder & Managing Partner, Monk's Hill Ventures

Expert Interviewees (continued)

Mr Lawrence Goh	Managing Director and COO of Group Technology & Operations, UOB Group
Prof Lam Kwok Yan	Executive Director, the Strategic Centre for Research in Privacy-Preserving Technologies and Systems (SCRiPTS), NTU
Mr Lee Ser Yen	Partner, Cybersecurity, KPMG
Ms Lien Huiluen	Director, Marketing and Strategic Partnerships, Sensetime
Mr Lih Shiun Goh	Senior Director for Public Affairs, Tencent
Mr Linden Reko	Cyber Advisor - Cyber Practice Asia, Marsh
Ms Lisa Mansour	Director, Product Management (Consulting, Insights & Analytics, Data Management), Mastercard
Mr Lokesh Bangalore	Vice President, Security and Compliance, Salesforce
Mr Lucius Lee	Senior Policy Lead, Product and Content, Aaqua
Admiral Mike Rogers	Senior Advisor, Brunswick Group
Dr Ming Tan	Founding Executive Director, Tech for Good Institute
Mr Minn Naing Oo	Managing Director and Partner, Allen & Gledhill
Mr Nabil Hamzi	Chief Product Security Architect, Logitech
Mr Nicholas Fang	Managing Director, Black Dot Research
Mr Nick Pan	Head of Recruitment, Tik Tok
Mr Paddy McGuiness, CMG OBE	Senior Advisor, Brunswick
Mr Rajat Maheshwari	Vice President, Digital Identity and Biometrics, Mastercard
Mr Rajeev Tummala	Director, Digital & Data, Markets & Securities Services, HSBC
Dr Raymond Chan	Expert AIOps Engineer, SAP
Mr Raymund Liboro	Commissioner and Chairman, National Privacy Commission (Philippines)
Mr Shameek Kundu	Head of Financial Services and Chief Strategy Officer, Truera
Prof Simon Chesterman	Dean, Faculty of Law, National University of Singapore
Mr Simon Gordon	Chief Commercial Officer, Accredify
Ms Siobhan Gorman	Partner, Crisis, Cybersecurity, Public Affairs and Media Relations, Brunswick Group
Mr Steven Koh	Director, Government Digital Services, GovTech
Ms Sunitha Chalam	Partner, Cybersecurity & Data Privacy Asia Pacific Lead, Brunswick Group
Mr Thomas Tay	Assistant Director, Product, IMDA
Mr Traven Teng	International Talent Acquisition Lead, Tencent
Ms Veronica Tan	Director, Safer Cyberspace, CSA
Ms Wan Wei Soh	Co-Founder & CEO, IKIGUIDE Metaverse Collective
Ms Wendy Lim	Partner, Cybersecurity Consulting, KPMG
Prof Jason Yap Chin Huat	Dean & Vice Provost, Practice, NUS
Mr Yeong Zee Kin	Deputy Commissioner, Personal Data Protection Commission
Ms Yvonne Lim	Director, Business and Ecosystems, IMDA

We would also like to put on record our thanks to the following organisations for supporting this study: Enterprise Singapore; our Presenting Sponsors Amazon Web Services (AWS) and NetSfere; our supporting sponsors Intel, Lenovo and Microsoft; and Eden Strategy Institute for their dedicated support in the industry consultation and research process.

12 References

[1]Infocomm Media Development Authority (IMDA). (2020). *Singapore grows trust in the digital environment.* Retrieved from https://www.imda.gov.sg/news-and-events/Media-Room/Media-Releases/2022/Singapore-grows-trust-in-the-digital-environment

[2]Personal Data Protection Commission Singapore (PDPC). (2020). *Model Artificial Intelligence Governance Framework Second Edition.* Retrieved from https://www.imda.gov.sg/news-and-events/Media-Room/Media-Releases/2022/Singapore-grows-trust-in-the-digital-environment

[3]POFMA Office. (2019). *Protection from Online Falsehoods and Manipulation Act (POFMA).* Retrieved from https://www.pofmaoffice.gov.sg/regulations/protection-from-online-falsehoods-and-manipulation-act/

[4]PDPC Singapore. (n.d.). *Data Protection Officers.* Retrieved from https://www.pdpc.gov.sg/overview-of-pdpa/data-protection/business-owner/data-protection-officers

[5]GovTech Singapore. (2021). *All Government Agencies to Accept Singpass Digital IC from 1 November 2021.* Retrieved from https://www.tech.gov.sg/media/media-releases/2021-10-28-all-government-agencies-to-accept-singpass-digital-ic-from-1-november-2021

[6]The Association of Banks in Singapore (ABS). (2021). *Data Sharing Handbook: For Banks and Non-Bank Data Ecosystem Partners.* Retrieved from https://www.tech.gov.sg/media/media-releases/2021-10-28-all-government-agencies-to-accept-singpass-digital-ic-from-1-november-2021

[7]Ritter, J. (2019). *What is digital trust?* Tech Target. Retrieved from https://www.techtarget.com/whatis/definition/digital-trust

[7]Chakravorti, B., Bhalla, A., & Chaturvedi, R. (2018). *The 4 Dimensions of Digital Trust, Charted Across 42 Countries.* Harvard Business Review. Retrieved from https://hbr.org/2018/02/the-4-dimensions-of-digital-trust-charted-across-42-countries

[7]PricewaterhouseCoopers (PWC). (2019). *The Journey To Digital Trust 2019* [E-book]. Retrieved from https://www.pwc.com/sg/en/publications/assets/the-journey-to-digital-trust-2019.pdf

[7]World Economic Forum (WEF). (2022). *Digital Trust.* Retrieved from https://www.weforum.org/projects/digital-trust

[7]Klynveld Peat Marwick Goerdeler (KPMG). (2015). *What is Digital Trust* [E-book]. Retrieved from https://assets.kpmg/content/dam/kpmg/pdf/2015/12/digital-trust.pdf

[7]Raviprakash, R. (2020). *What is Digital Trust?.* Subex Limited. Retrieved from https://www.subex.com/blog/what-is-digital-trust/

[7]Allan, A., Zlotogorski, M., Gaehtgens, F., & Buytendijk, F. (2017). *Definition: Digital Trust.* Retrieved from https://www.gartner.com/en/documents/3727718/definition-digital-trust

[7]Hitachi. (2020). *Understanding Digital Trust.* Retrieved from https://www.hitachi.com/rd/sc/ai-analytics/003/index.html.

[7]Swinhoe, D. (2018). *What is digital trust?* How CSOs can help drive business. Retrieved from https://www.csoonline.com/article/3297037/what-is-digital-trust-how-csos-can-help-drive-business.html

[7]ISACA. (2022). *State of Digital Trust 2022*. Retrieved from https://www.isaca.org/-/media/files/isacadp/project/isaca/resources/reports/state-of-digital-trust-2022-report-final.pdf

[7]Zahn, N., & Paeffgen, N. (2022). *Digital Trust Whitepaper. Swiss Digital Initiative.* Retrieved from https://a.storyblok.com/f/72700/x/7bd8e2fe21/digital-trust-whitepaper.pdf

[8]Shuklar, A.K. (2021). *India leads the global e-governance race with 1.3 bn digital ID users.* Economic Times (ET) Government. Retrieved from https://government.economictimes.indiatimes.com/news/digital-india/india-leads-the-global-e-governance-race-with-1-3-bn-digital-id-users/90789137

[9]European Parliamentary Research Service (EPRS). (2022). *Updating the European digital identity framework.* Retrieved from https://www.europarl.europa.eu/RegData/etudes/BRIE/2021/698772/EPRS_BRI(2021)698772_EN.pdf

[10]Zheng, W. (2022). *China plans digital version of national identification card later this year, premier says.* South China Morning Post (SCMP). Retrieved from https://www.scmp.com/news/china/politics/article/3170214/china-plans-digital-version-national-identification-card-later

[11]Edelman Research. (2022). *Edelman Trust Barometer 2022* [E-book]. Retrieved from https://www.edelman.com/sites/g/files/aatuss191/files/2022-01/2022%20Edelman%20Trust%20Barometer%20FINAL_Jan25.pdf

[12]Edelman Research. (2021). *Edelman Trust Barometer 2021* [E-book]. Retrieved from https://www.edelman.com/sites/g/files/aatuss191/files/2021-03/2021%20Edelman%20Trust%20Barometer.pdf

[13]Edelman Research. (2021). Edelman Trust Barometer 2021 [E-book]. Retrieved from https://www.edelman.com/sites/g/files/aatuss191/files/2021-03/2021%20Edelman%20Trust%20Barometer.pdf

[14]Imperva. (2022). *Imperva Bad Bot Report* [E-book]. Retrieved from https://www.imperva.com/resources/reports/2022-Imperva-Bad-Bot-Report.pdf

[15]Ipsos. (2019). *CIGI-IPSOS Global Survey: Internet Security & Trust, 2019 Part 3: Social Media, Fake News & Algorithms.* [E-book]. Retrieved from https://www.cigionline.org/sites/default/files/documents/2019%20CIGI-Ipsos%20Global%20Survey%20-%20Part%203%20Social%20Media%2C%20Fake%20News%20%26%20Algorithms.pdf

[16]Tandoc, E., Goh, Z., & Lee, E. (2022). *Digital Life During a Pandemic, Results from a Panel Study.* Nanyang Technological University Singapore. Retrieved from https://www.ntu.edu.sg/docs/librariesprovider127/default-document-library/in-cube-working-paper-no.1.pdf?sfvrsn=442c20003

[17]Ipsos. (2019). *CIGI-IPSOS Global Survey: Internet Security & Trust, 2019 Part 3: Social Media, Fake News & Algorithms.* [E-book]. Retrieved from https://www.cigionline.org/sites/default/files/documents/2019%20CIGI-Ipsos%20Global%20Survey%20-%20Part%203%20Social%20Media%2C%20Fake%20News%20%26%20Algorithms.pdf

[18]Imperva. (2022). *Imperva Bad Bot Report* [E-book]. Retrieved from https://www.imperva.com/resources/reports/2022-Imperva-Bad-Bot-Report.pdf

[19]POFMA Office. (2019). *Protection from Online Falsehoods and Manipulation Act (POFMA)*. Retrieved from https://www.pofmaoffice.gov.sg/regulations/protection-from-online-falsehoods-and-manipulation-act/

[20]Confessore, N. (2018). *Cambridge Analytica and Facebook: The Scandal and the Fallout So Far.* The New York Times. Retrieved from https://www.nytimes.com/2018/04/04/us/politics/cambridge-analytica-scandal-fallout.html

[21]Buranyi, S. (2017). *Rise of the racist robots – how AI is learning all our worst impulses.* The Guardian. Retrieved from https://www.theguardian.com/inequality/2017/aug/08/rise-of-the-racist-robots-how-ai-is-learning-all-our-worst-impulses

[22]United Nations Conference on Trade and Development (UNCTAD). (n.d.). *Data Protection and Privacy Legislation Worldwide.* Retrieved from https://unctad.org/page/data-protection-and-privacy-legislation-worldwide

[23]United Nations Conference on Trade and Development (UNCTAD). (2021). *Data Protection and Privacy Legislation Worldwide.* Retrieved from https://unctad.org/page/data-protection-and-privacy-legislation-worldwide

[24]China Briefing (2021). *The PRC Personal Information Protection Law (Final): A Full Translation.* Retrieved from https://www.china-briefing.com/news/the-prc-personal-information-protection-law-final-a-full-translation/

[25]SC Media (2022). *California Privacy Rights Act (CPRA) compliance checklist: What you need to know.* Retrieved from https://www.scmagazine.com/native/incident-response/california-privacy-rights-act-cpra-compliance-checklist-what-you-need-to-know

[26]Singapore Computer Society (2020). *AI Ethics and Governance Body of Knowledge.* Retrieved from https://www.scs.org.sg/ai-ethics-bok

[27]The Organisation for Economic Co-operation and Development (OECD) (2022). *OECD AI's Live Repository of AI Strategies & Policies.* Retrieved from https://oecd.ai/en/dashboards

[28]United Nations Conference on Trade and Development (UNCTAD). (2021). *Data Protection and Privacy Legislation Worldwide.* Retrieved from https://unctad.org/page/data-protection-and-privacy-legislation-worldwide

[29]Cavoukain, A. (2011). *Privacy by Design, The 7 Foundational Principles, Implementation and Mapping of Fair Information Practices.* Information and Privacy Commissioner of Ontario. Retrieved from https://iapp.org/media/pdf/resource_center/pbd_implement_7found_principles.pdf

[30]Morgan, S. (2020). *Cybercrime To Cost The World $10.5 Trillion Annually By 2025.* Cybercrime Magazine. Retrieved from https://cybersecurityventures.com/cybercrime-damages-6-trillion-by-2021/

[31]Morgan, S. (2019). *Global Ransomware Damage Costs Predicted To Reach $20 Billion (USD) By 2021. Cybercrime Magazine.* Retrieved from https://cybersecurityventures.com/global-ransomware-damage-costs-predicted-to-reach-20-billion-usd-by-2021/

[32]Wilkie, C. (2021). *Colonial Pipeline paid $5 million ransom one day after cyberattack, CEO tells Senate.* CNBC. Retrieved from https://unctad.org/page/data-protection-and-privacy-legislation-worldwide

[33]Check Point Software. (2021). *Check Point Research: Asia Pacific experiencing a 168% year on year increase in cyberattacks in May 2021.* Retrieved from https://blog.checkpoint.com/2021/05/27/check-point-research-asia-pacific-experiencing-a-168-year-on-year-increase-in-cyberattacks-in-may-2021/

[34]Statista Research Department. (2022). *Cybercrime as a share of total crimes in Singapore from 2014 to 2021.* Retrieved from https://www.statista.com/statistics/1267252/singapore-cybercrime-as-share-of-total-crime/#:~:text=Cybercrime%20as%20share%20of%20total%20crime%20Singapore%202014%2D2021&text=In%202021%2C%20-cybercrime%20made%20up,crimes%20committed%20in%20the%20country

[35]Morgan, S. (2020). *Cybercrime To Cost The World $10.5 Trillion Annually By 2025.* Cybercrime Magazine. Retrieved from https://cybersecurityventures.com/cybercrime-damages-6-trillion-by-2021/

[36]Walter, J. (2020). *COVID-19 News: FBI Reports 300% Increase in Reported Cybercrimes.* IMC Grupo. Retrieved from https://www.imcgrupo.com/covid-19-news-fbi-reports-300-increase-in-reported-cybercrimes/

[37]Check Point Software. (2021). *Check Point Research: Asia Pacific experiencing a 168% year on year increase in cyberattacks in May 2021.* Retrieved from https://blog.checkpoint.com/2021/05/27/check-point-research-asia-pacific-experiencing-a-168-year-on-year-increase-in-cyberattacks-in-may-2021/

[38]Ganesan, N. (2022). *Singapore faced more cybercrime, phishing and ransomware threats in 2021.* Channel News Asia (CNA). Retrieved from https://www.channelnewsasia.com/singapore/cybercrime-ransomware-phishing-cybersecurity-2021-2906386

[39]Cyber Security Agency of Singapore (CSA). (2022). *Cyber Trust Mark*. Retrieved from https://www.csa.gov.sg/Programmes/sgcybersafe/cybersecurity-certification-for-enterprises/cyber-trust-mark

[40]Cory, N. & Dascoli, L. (2021). *How Barriers to Cross-Border Data Flows Are Spreading Globally, What They Cost, and How to Address Them* [E-book]. Information Technology & Innovation Foundation. Retrieved from https://www2.itif.org/2021-data-localization.pdf

[41]Cory, N. & Dascoli, L. (2021). *How Barriers to Cross-Border Data Flows Are Spreading Globally, What They Cost, and How to Address Them* [E-book]. Information Technology & Innovation Foundation. Retrieved from https://www2.itif.org/2021-data-localization.pdf

[42]Yan, L., Yu, Z., & Liu, V. (2021). *The future of data localization and cross-border transfer in China: a unified framework or a patchwork of requirements?* Financial Crimes Enforcement Network. Retrieved from https://www.fincen.gov/resources/statutes-regulations/usa-patriot-act

[43]Greenwalf, G., MacAskill, E., & Poitras, L. (2013). *Edward Snowden: the whistleblower behind the NSA surveillance revelations.* The Guardian. Retrieved from https://www.theguardian.com/world/2013/jun/09/Edward-snowden-nsa-whistleblower-surveillance

[44]Financial Crimes Enforcement Network. (n.d.). *USA Patriot Act.* Retrieved from https://www.fincen.gov/resources/statutes-regulations/usa-patriot-act

[45]International Association of Privacy Professionals (IAPP) & Ernst & Young (EY) (2021). *IAPP-EY Annual Privacy Governance Report 2021* [E-book]. Retrieved from https://iapp.org/media/pdf/resource_center/IAPP_EY_Annual_Privacy_Governance_Report_2021.pdf

[46]IAPP & EY. (2021). IAPP-EY Annual Privacy Governance Report 2021 [E-book]. Retrieved from https://iapp.org/media/pdf/resource_center/IAPP_EY_Annual_Privacy_Governance_Report_2021.pdf

[47]Association of Southeast Asian Nations (ASEAN). (2021). *ASEAN Model Contractual Clauses for Cross Border Data Flows.* Retrieved from https://asean.org/wp-content/uploads/3-ASEAN-Model-Contractual-Clauses-for-Cross-Border-Data-Flows_Final.pdf

[48]Finlayson-Brown, J. (2022). *New Global Cross-Border Privacy Rules Forum established by APEC CBPR members.* Allen & Overy. Retrieved from https://www.allenovery.com/en-gb/global/blogs/digital-hub/new-global-cross-border-privacy-rules-forum-established-by-apec-cbpr-members

[49]Mastercard. (2019). *Restoring Trust in a Digital World.* Retrieved from https://www.mastercard.us/content/dam/mccom/en-us/issuers/digital-identity/digital-identity-restoring-trust-in-a-digital-world-final-share-corrected.pdf

[50]Bank for International Settlements (BIS). (2022). *Project Dunbar: International settlements using multi-CBDCs.* Retrieved from https://www.mas.gov.sg/-/media/MAS-Media-Library/development/fintech/Dunbar/Project_Dunbar_Report_2022.pdf

[51]Association of Southeast Asian Nations (ASEAN). (2021). *2021 ADGSOM Project Completion Report: Blockchain for digital government – the ASEAN way* [E-book]. Retrieved from https://asean.org/wp-content/uploads/2022/02/02-Final-_-Report-Blockchain-for-digital-government.pdf

[52]Bigg, C., Lee, Y. L., & To, G. (2022). *Singapore: Higher Fines for Breach of Personal Data Protection Act 2012 (PDPA) – up to 10% of Singapore Turnover.* Bank for International Settlements (BIS). Retrieved from https://blogs.dlapiper.com/privacymatters/singapore-higher-fines-for-breach-of-personal-data-protection-act-2012-pdpa-up-to-10-of-singapore-turnover/

[53]Wolford, B. (2019). *What are the GDPR Fines?* GDPR.eu. Retrieved from https://gdpr.eu/fines/

[54]Morgan, S. (2021). *Cybersecurity Jobs Report: 3.5 Million Openings In 2025.* Cybercrime Magazine. Retrieved from https://cybersecurityventures.com/jobs/

[55]Polaris Market Research (2021). *Enterprise Governance, Risk & Compliance Market Share, Size, Trends, Industry Analysis Report, By Component (Software, Services); By Software (Audit Management, Compliance Management, Risk Management, Policy Management, Incident Management, Others); By Services; By Vertical; By Region; Segment Forecast, 2021 – 2028.* Retrieved from https://www.polarismarketresearch.com/industry-analysis/enterprise-governance-risk-compliance-egrc-market

[56]International Data Corporation (IDC) (2021). *IDC Forecasts Solid Growth for GRC Solutions as Enterprises Invest to Expand and Integrate Their Governance and Risk Management Portfolios.* Retrieved from https://www.idc.com/getdoc.jsp?containerId=prUS48171921

SGTech, which celebrated its 40th anniversary in 2022, is the leading trade association for Singapore's tech industry. Representing over 1,000 member companies ranging from top multinational corporations, large local enterprises, vibrant small and medium-sized enterprises, and innovative startups, it is the largest community in Singapore where companies converge to advocate for change and drive what enables tech innovation and accelerates tech adoption to spur greater sustainability in the sector.

SGTech's mission is to catalyse a thriving ecosystem that powers Singapore as a global tech powerhouse.

Get in Touch

SGTech - through its Digital Trust Committee - is spearheading many initiatives towards positioning Singapore as a global node for digital and data, built on trust. Interest in our work on Digital Trust among our membership is growing rapidly and we welcome collaboration from all stakeholders in the tech ecosystem, whether from industry, government or the non-profit sector.

Contact us if you would like to learn more on how to be part of our Digital Trust journey, or if you wish to find out more about the complete Digital Trust Landcape Study.

research@sgtech.org.sg

sgtech.org.sg
SGTech
SGTech
research@sgtech.org.sg