National Digital Identity and Government Data Sharing in Singapore

A Case Study of Singpass and APEX

THE WORLD BANK
IBRD • IDA | WORLD BANK GROUP

ID4D
IDENTIFICATION FOR DEVELOPMENT

GOVTECH
SINGAPORE

1818 H Street, NW, Washington, D.C., 20433
Telephone: 202-473-1000; Internet: www.worldbank.org

This work is a product of the staff of The World Bank with external contributions. The findings, interpretations, and conclusions expressed in this work do not necessarily reflect the views of The World Bank, its Board of Executive Directors, or the governments they represent. The World Bank does not guarantee the accuracy of the data included in this work. The boundaries, colors, denominations, and other information shown on any map in this work do not imply any judgment on the part of The World Bank concerning the legal status of any territory or the endorsement or acceptance of such boundaries.

Nothing herein shall constitute or be considered to be a limitation upon or waiver of the privileges and immunities of The World Bank, or of any participating organization to which such privileges and immunities may apply, all of which are specifically reserved.

Rights and Permission

CONTENTS

Table of Figures

Table of Boxes

Table of Tables

ABOUT ID4D

The World Bank Group's Identification for Development (ID4D) initiative combines global knowledge, cross-sectoral expertise, financial and technical assistance, and partnerships to help countries realize the transformational potential of identification and civil registration. The goal of ID4D is to accelerate inclusive growth and the achievement of a wide range of development outcomes by enabling all people to exercise their rights and to access more and better services. The work of ID4D is made possible through support from the Bill & Melinda Gates Foundation, the Norwegian Agency for Development Cooperation, the Omidyar Network, and the governments of France and the United Kingdom

To find out more about ID4D, visit **https://id4d.worldbank.org/**

ACKNOWLEDGEMENTS

This case study was authored by Adam Cooper, under the supervision of Jonathan Marskell (World Bank) and Cheow Hoe Chan (Singapore Government Technology Agency). It is the result of collaboration between The World Bank Group's Identification for Development (ID4D) Initiative and Singapore's Government Technology Agency (GovTech) to share knowledge and experiences for the benefit of other countries.

Excellent feedback and input were provided throughout the development of this case study. We thank the following individuals for their various contributions: Dominic Chan, Kendrick Lee, Lynette Kwok, Kok Khuan Fong, Li Ting Guo, Yoke May Kam, Hazel Koh, Karen Kee, Billy Teo, Wan Yieng Chong, Vithya Selvam, and Adrian Chan (GovTech); and Vyjayanti Desai, Julia Clark, Faher Elfayez, Marie Eichholtzer, Burak Eskici, and Carla Berisso Queirolo (World Bank). We also appreciate peer reviews by Quek Sin Kwok (formerly of GovTech), Hsiao Ming Chia (GovTech), Junko Narimatsu (World Bank), and Khuram Farooq (World Bank). Screenshots of the Singpass application are from the Singpass website: https://www.singpass.gov.sg/

ABBREVIATIONS

2FA	Two-Factor Authentication
APEX	API Exchange (APEX)
API	Application Programming Interface
ASEAN	Association of Southeast Asian Nations
AU	APEX Units
CDA	Child Development Account
CODEX	Core Operations Development Environment and eXchange
CPF	Central Provident Fund
CWC	Cyber Watch Centre
DGB	Digital Government Blueprint
EASY	E-Services Authorisation System
eBLs	Electronic Bills of Lading
FIN	Foreign Identification Number
G2B	Government-to-Business
G2C	Government-to-Citizens
GCC	Government on Commercial Cloud
GDS	Government Digital Services
GovTech	Government Technology Agency
HTX	Home Team Science and Technology Agency
IC	ID Card
ICA	Immigration and Checkpoints Authority
ICT	Information and Communication Technologies
IDA	Infocomm Development Authority of Singapore
IRAS	Inland Revenue Authority of Singapore

ISO	International Organization for Standardization
JWT	JSON Web Token
JWKS	JSON Web Key Set
KYC	Know Your Customer
MAS	Monetary Authority of Singapore
MCI	Ministry of Communication and Information
mDL	Mobile driving license
MHA	Ministry of Home Affairs
MLETR	Model Law on Electronic Transactions Act
MOF	Ministry of Finance
MOM	Ministry of Manpower
MTI	Ministry of Trade and Industry
NCA	National Certificate Authority
NCB	National Computer Board
NDI	National Digital Identity
NFC	Near-Field Communication
NRIC	National Registration Identity Card
NTC	National Translation Committee
OIDC	Open ID Connect
OP	OpenID Provider
PDPC	Personal Data Protection Commission
PKI	Public Key Infrastructure
PMO	Prime Minister's Office
SGFinDex	Singapore Financial Data Exchange
SGTraDex	Singapore Trade Data Exchange
SGTS	Singapore Government Technology Stack
SIEM	Security Information and Event Management
SII	Significant Information Infrastructure
SNDGG	Smart Nation and Digital Government Group
SNDGO	Smart Nation and Digital Government Office
SNPO	Smart Nation Programme Office

SPF	Singapore Police Force
TPS	Transactions-per-Second
UEN	Unique Entity Number
UNCITRAL	United Nations Commission on International Trade Law
URI	Uniform Resource Identifier
VM	Virtual Machine
WOG	Whole-of-Government

Key Definitions

Credential A document, object, or data structure that vouches for the identity of a person or other entity through some method of trust and authentication

Digital Public Infrastructure (DPI) Solutions and systems that enable the effective provision of essential, society-wide functions and services in the public and private sectors, such as digital identification, digital payments, and data sharing.

Foundational ID ID systems primarily created to manage identity information for the general population and provide credentials that serve as proof of identity for a wide variety of public and private sector transactions and services. Common types of foundational ID systems include civil registries, national ID systems, and population registers.

Relying Party (RP) An entity that relies upon the credentials and authentication mechanisms provided by an ID system, typically to process a transaction or grant access to information or a to system

Selective Disclosure The ability of a user to make nuanced decisions about what information to share.

Trust Framework A set of operational, business, and technical rules and associated governance to enable a group of entities (including schemes) to interoperate with an adequate level of trust.

User The entity in control of a credential.

EXECUTIVE SUMMARY

The ability of an individual to reliably prove their identity is crucial to ensure access to services and exercise rights. The foundational ID systems that enable people to do this also help government agencies and businesses to improve how services are delivered, streamline processes, and reduce leakages and fraud. As countries digitalize, and the number and importance of end-to-end online transactions grow, the mechanisms used to prove identity in the physical world are not as reliable in the digital world. Digital ID systems, which allow people to prove their officially recognized identity online and without a physical interaction, have therefore become key enabler for the inclusive digital transformation of countries.

Similarly, as highlighted in the 2021 World Development Report, Data for Better Lives, governments can be better at responding to the needs of citizens and businesses by being able to seamlessly and securely exchange data.[1] Such data re-use can not only increase the efficiency of government services and operations; it can also unlock innovation by the private sector, civil society, and individuals. It is for this reason that governments around the world have built data sharing platforms of various types, including with linkages to digital identity to enable people to exercise consent and control over their personal data.

This case study describes Singpass, Singapore's national digital identity (NDI), and API Exchange (APEX), the government's data sharing platform. It highlights not just how they work but also how they work together. Built by the Government Technology Agency of Singapore (GovTech), both products have helped to improving the lives of Singaporeans and residents, and to enabling government agencies and businesses to offer better services. This has contributed greatly to Singapore becoming a leading digital government, economy, and society, which are the three pillars of its Smart Nation Initiative.

The section on Singpass, which began in 2003 simply as a username and password login system to access government websites, shows how it has evolved over time. This is an important characteristic of its success, as Singapore has not attempted to build a new identity system, but rather to create a digital version of the foundational ID system that people use in their everyday life. This experience

[1] World Bank, 2021. *World Development Report 2021: Data for Better Lives*. https://www.worldbank.org/en/publication/wdr2021

offers important lessons and may be adapted by other countries with equally strong foundational ID systems, bearing in mind the need to design for local political, legal, social, and economic conditions.

The success of Singpass is evident in its adoption. 97 percent of the eligible population (or 4.5 million citizens and residents) uses the Singpass application to access more than 2,000 public and private sector services online, ranging from financial services to healthcare, education, business services, and transportation. More than 350 million transactions are completed each year, and transactions that previously took days or hours to complete, often requiring physical visits, now take minutes and can be performed from anywhere with an internet connection. A document wallet has recently been added, enabling citizens and residents to store their identity cards, driving license, and COVID-19 vaccination documentation—and more documents will soon be added. This document wallet is accessed more than 300,000 times a month and is growing in popularity.

Singpass also empowers Singaporeans and residents to provide consent to sharing their data held in government databases via the Myinfo product. This has led to reductions in the cost and time for transactions with government agencies and businesses. Approximately 200,000 Myinfo transactions take place per day. The time it takes to apply for services using Myinfo has decreased by up to 80 percent, with businesses also reporting significant cost savings and up to a 15 percent higher approval rating from their customers.

The section on APEX, which is an application programming interface (API) gateway for government agencies to share and re-use data transparently, securely and seamlessly, shows how it has enabled public services to be more efficient. For example, APEX is a key backbone for the functioning of Singpass, including onboarding (validating information with the foundational ID system) and Myinfo transactions. The number of APIs supported through APEX has surpassed 2,000, from over 45 different agency projects, approximately half of all government agencies in Singapore. The level of traffic has surpassed 100 million transactions per month, with peaks on average exceeding 300 million transactions per month.

GovTech is constantly looking for ways to improve Singpass and APEX. Alternative models for Singpass are under consideration, including federated and decentralized architectures. Other plans include introducing authorization services for businesses, expanding the digital wallet, and establishing cross-border interoperability with other countries. Similarly, GovTech will be piloting the use of APEX within the private sector and will be moving non-sensitive functionalities to the cloud to improve scalability.

Any country wishing to build their own NDI and government data sharing platform should consider their own national requirements and may adapt or learn from the experience of Singapore (as well as other countries), rather than directly replicating their approach. Some key takeaways from the experience with Singpass and APEX include:

- Evolution: gradually improving products and services, based on experiences and lessons, rather than trying to solve too many problems at the same time.
- Prioritizing user experience: investing time and other resources across the development lifecycle to understand what users want and expect, especially among vulnerable users.
- Focusing on use cases: driving adoption by identifying where the most value will be generated.
- Identifying authoritative sources of data in government: developing common data standards and identifying the most reliable sources for each data attribute, rather than replicating information across databases.
- Technology and skillsets: adopting open technologies where appropriate and continuously investing in people.
- Responsibly adopting technologies: using new technologies when relevant rather than when they become available.

NDI and data exchange platforms are a key part (along with digital payments) of what has become known as digital public infrastructure (DPI), the solutions that enable the effective provision of essential society-wide functions and services in the public and private sectors. This case study highlights how Singapore has successfully developed its DPI to improve the lives and livelihoods of its citizens and residents and boost its economic competitiveness.

CALL FOR COLLABORATION

Countries and international organizations interested in collaborating with GovTech on NDI and government data sharing projects can contact GovTech via email at **info@tech.gov.sg**

1 INTRODUCTION

This case study describes Singapore's National Digital Identity (NDI) (known as Singpass and inclusive of its Myinfo personal data sharing consent product) and government data sharing platform (known as the API Exchange or APEX), which are digital public infrastructure (DPI) built and maintained by Singapore's Government Technology Agency (GovTech). It illustrates how Singpass, Myinfo, and APEX work together to improve the lives of Singapore's citizens and residents, as well as to boost Singapore's economic competitiveness, in accordance with Singapore's Smart Nation Initiative.

The objective of this case study is to help policymakers and practitioners in other countries to contextualise Singapore's experience and key takeaways as they design and implement their own NDI and government data sharing platforms.

1.1 Country Context

Singapore is a relatively small, high-income island city-state. In 2021, it had a population of nearly 5.5 million, which includes approximately 2 million non-national residents.[2] Recognizing the challenges and vulnerabilities of its size and lack of natural resources, the government has invested heavily in digital technologies as a driver of growth, competitiveness, and prosperity.

Internet access is reliable and widely available in Singapore. According to the 2021 Global Findex Survey**,** 98 percent of the population aged 15 and older has a financial account, and 97 percent has a mobile phone.[3] As described later in this case study, the country's foundational ID systems, including civil registration, have universal coverage.

This does not mean that other countries should be discouraged if they do not have all of these advantages. There is still much to learn from the Singaporean experience, and a rigid implementation of what has worked in Singapore will not be appropriate in other countries. It is the approach and lessons that are of primary value.

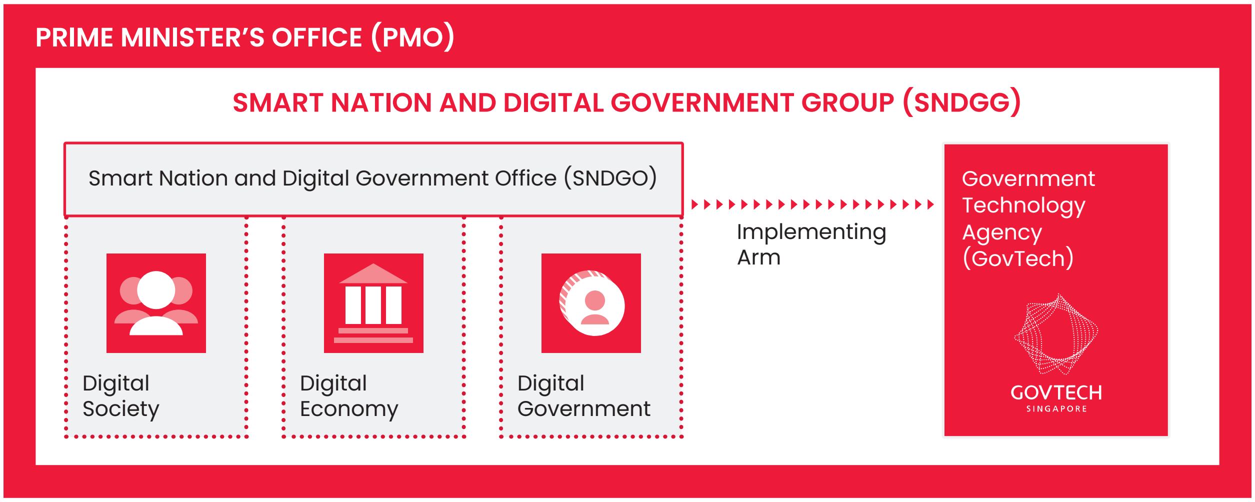
[2] Government of Singapore, 2021. *Population in Brief – 2021*. https://www.population.gov.sg/files/media-centre/publications/population-in-brief-2021.pdf

[3] World Bank, 2022. *The Global Findex Database 2021*. https://www.worldbank.org/en/publication/globalfindex

1.2 The Smart Nation Initiative

Launched in 2014 by Prime Minister Lee Hsien Loong, the Smart Nation Initiative is driven by the Smart Nation and Digital Government Group (SNDGG), which is housed in the Prime Minister's Office (PMO) and is comprised of the Smart Nation and Digital Government Office (SNDGO) for planning and policy functions and the Government Technology Agency (GovTech), which functions as the implementation arm (see figure 1.2.1).[4] The SNDGG is headed by a Permanent Secretary in the Prime Minister's Office and overseen by a Ministerial Committee.[5] The pillars for the Smart Nation Initiative are Digital Society, Digital Economy, and Digital Government.

Figure 1.2.1 Institutional Arrangements for the Smart Nation Initiative

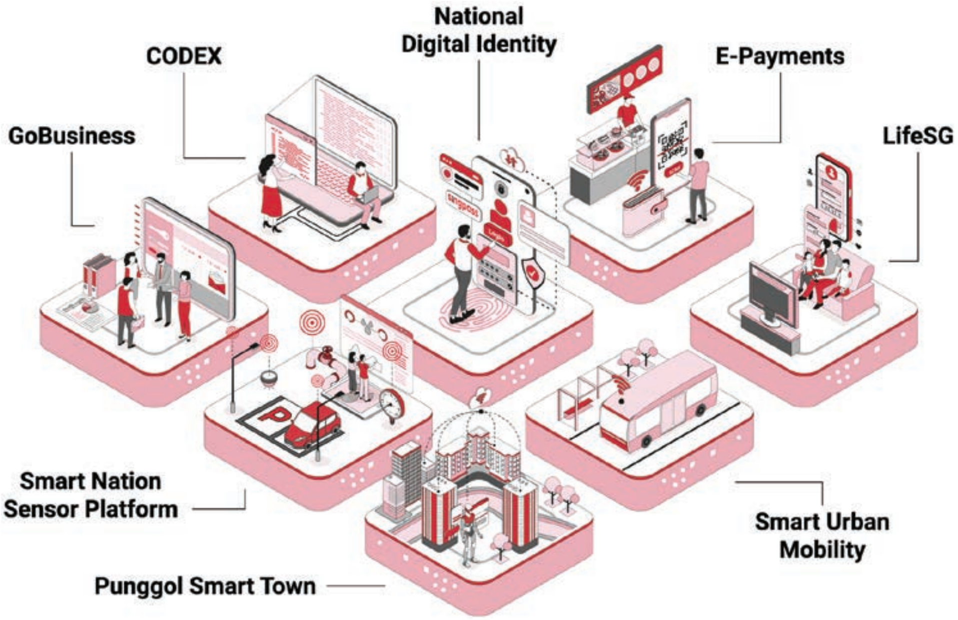

PRIME MINISTER'S OFFICE (PMO)
SMART NATION AND DIGITAL GOVERNMENT GROUP (SNDGG)
Smart Nation and Digital Government Office (SNDGO)
Digital Society
Digital Economy
Digital Government
Implementing Arm
Government Technology Agency (GovTech)
GOVTECH
SINGAPORE

The Smart Nation Initiative and SNDGG are critical success factors for Singpass (including Myinfo) and APEX. They provide a coherent and comprehensive over-arching policy and institutional framework, which enables whole-of-government (WOG) approaches, participation of the public, and collaboration with the private sector. Furthermore, by identifying strategic national projects (see figure 1.2.2), which include NDI for Singpass, and Core Operations Development Environment and eXchange (CODEX) for APEX, the Smart Nation Initiative provides clarity on priorities, facilitating the coordination and resourcing needed for successful delivery.

[4] For more information about Singapore's Smart Nation Initiative, see: https://www.smartnation.gov.sg/about-smart-nation/transforming-singapore

[5] Government of Singapore. 2022. "About Smart Nation Digital Government Group." https://www.smartnation.gov.sg/about-smart-nation/sndgg

Figure 1.2.2 Smart Nation Initiative Strategic National Projects[6]



1.3 Government Technology Agency (GovTech)

GovTech is a statutory board under the PMO that is responsible for digital transformation within the public sector. It was established in 2016 under the Ministry of Information and Communication as a successor to the Infocomm Development Authority of Singapore (IDA), before moving to the PMO in 2017. In July 2022, GovTech employed approximately 3,400 staff members and in 2021 had a budget of SG$635.5 million. The Government Chief Digital Technology Officer concurrently serves as GovTech's Deputy Chief Executive Officer.

GovTech's work can be broadly classified into three areas:

- **Products:** More than 700 in-house developers build products for citizens, such as Singpass and Myinfo; businesses, including Corppass; and the WOG, such as APEX. This also includes capability centres—for example, on data science and artificial intelligence—and WOG infrastructure, for example: the government on commercial cloud systems. GovTech also spearheads strategic national projects.
- **Services:** Making up more than half of GovTech's staff, the Services group manages technology across over 60 percent of Singapore's government agencies.
- **Cybersecurity and Governance:** GovTech is the sector lead for cybersecurity in the Singapore government, responsible for setting WOG policies and guidelines to ensure the safety and security of government digital structures.

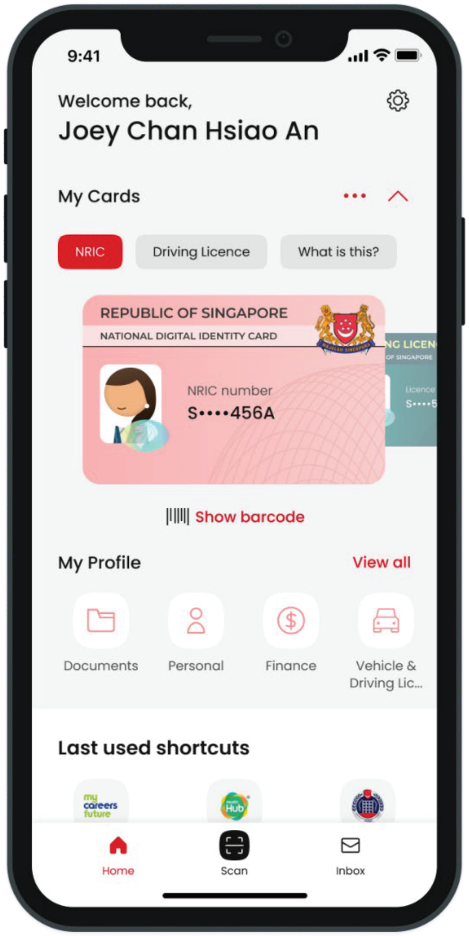
[6] Government of Singapore, n.d. *Smart Nation Initiative – Our Strategic National Projects.* https://www.smartnation.gov.sg/initiatives/strategic-national-projects

2 SINGAPORE’S NATIONAL DIGITAL IDENTITY: singpass

2.1 Overview of Singpass

Singpass comprises the smartphone application and a back-end managed by GovTech. The smartphone application is the user-facing component, which is accessible for free to all Singapore citizens, permanent residents, and Foreign Identification Number (FIN) holders aged 15 and older. It enables users to leverage their legal identity to carry out a wide range of online and face-to-face transactions with government agencies and businesses. Singpass was first launched in 2003 as a username and password to sign into government websites and has since significantly evolved.

Figure 2.1 Singpass Home Screen



Welcome back,
Joey Chan Hsiao An

REPUBLIC OF SINGAPORE
NATIONAL DIGITAL IDENTITY CARD
NRIC number
S••••456A

Today, Singpass includes several products and features for citizens and residents, including:

- **Login:** Users can verify their identity online in a secure and trusted manner when transacting with websites and smartphone applications of government agencies and businesses. Verification can be performed using a six-digit PIN code or the phone unlock mechanism, such as a fingerprint or selfie, on most devices.
- **Verify:** User identity is verified for a face-to-face transaction and the secure transfer of personal information through scanning of QR codes or tapping near-field communication (NFC) devices.
- **Myinfo:** Manages the use and sharing of personal data for simpler online transactions; data is pulled in real time from authoritative sources, and consent is facilitated through Login or Verify. For example, this feature can be used to pre-fill forms.
- **Identiface:** A stronger method of authentication than Login or Verify that uses face verification based on the latest facial image enrolled with the Immigration and Checkpoints Authority (ICA).

- **Digital IC:** Enables users to present a digital version of their National Registration Identity Card (NRIC) or FIN card.
- **Sign:** Users can create secure electronic signatures using a preferred third party digital signing tool compliant with Singapore's Electronic Transactions Act.
- **Document Wallet:** Users can store digital versions of other official documents, such as a driving license and HealthCerts (including COVID-19 vaccination certificates).
- **Notify:** This feature enables users to receive push notifications and alerts from government agencies, as well as information related to Singpass transactions.
- **Shortcuts:** Users are able to log in directly to commonly used digital government services, such as the Central Provident Fund (CPF) for social security, HealthHub for health services and records, and the Inland Revenue Authority of Singapore (IRAS) MyTax Portal.

Singpass also functions as a digital ID for legal entities. Eligible owners and officers of businesses and other entities (such as non-profit organizations and associations) can use **Login** and **Myinfo business** on behalf of a legal entity when accessing digital government services. Roles and user rights are managed through the Corppass website.

The Singpass application is available on Apple iOS, Android, and Huawei devices. Singpass, including the application and back-end, uses various technologies, including cryptography and biometrics, for convenience, security, and trust. Relying parties (RPs) can integrate with Singpass using NDI application programming interfaces (APIs). More than 85 percent of all Singpass transactions are conducted through the application, with the remaining 15 percent using two-factor authentication (2FA) methods, such as Singpass's Identiface (including through a web browser).

2.2 Singapore's Foundational ID System as a Basis for Singpass

An important characteristic of Singpass as a *digital* ID is how it functions as an extension of, and builds on, Singapore's foundational ID system. The information in the foundational ID system is used by Singpass, including for onboarding—that is, verifying identity when initially creating the digital ID; for the digital identity card (IC); and for face verification, known as Identiface. The availability of this information and the means to easily verify it made the transition to NDI relatively straightforward. Furthermore, the issuance of a unique identifier and the existence of a national registry of persons as an authoritative source of core demographic attributes facilitate interoperability. This and the subsequent WOG approach to data are key success factors for Myinfo and API Exchange (APEX). Box 2.2.1 describes additional use cases for NRIC numbers and FINs and how these unique identifiers are protected against misuse.

Box 2.2.1 Additional Use Cases and Protections for National Registration Identity Card (NRIC) Numbers and Foreign Identification Numbers (FIN)

Since 2017, NRIC numbers and FINs (along with mobile phone numbers) can be linked to a person's bank account and used as a payment address, using the PayNow real-time payment system.

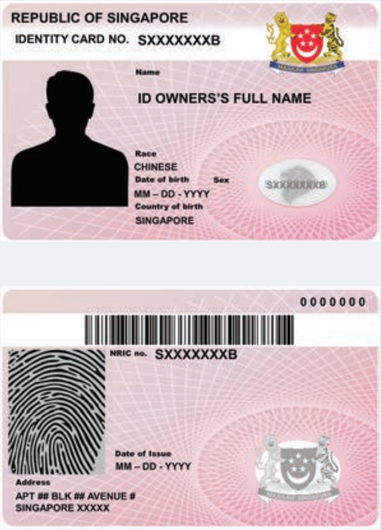
In recognition of the data protection risks surrounding permanent unique identifiers, in 2018, the Personal Data Protection Commission (PDPC) issued advisory guidelines on the Personal Data Protection Act for NRIC and other national identification numbers. Under these advisory guidelines, private sector organizations can only collect NRIC, FIN, and other identification numbers if it is required by law, or if it is necessary to establish or verify an individual's identity to a high degree of accuracy.[7]

The Immigration and Checkpoints Authority (ICA), under the Ministry of Home Affairs (MHA), is responsible for Singapore's foundational ID system, including civil registration, in accordance with Singapore's National Registration Act. This is in addition to responsibilities for border management and passport issuance. The Ministry of Manpower (MOM) is responsible for the registration of work pass holders. An NRIC number is issued at birth registration for citizens, and a FIN is issued to foreigners when they register for a long-term pass, such as permanent resident status or a work pass.

[7] Personal Data Protection Commission Singapore. n.d. "NRIC FAQs." https://www.pdpc.gov.sg/NRIC-faqs

At the age of 15, citizens and permanent residents must report to an ICA premise to enrol their fingerprints, irises, and a facial image when they are issued a physical identity card (IC); ICA introduced irises as an additional biometric modality in 2017. Fingerprints and irises are used for both deduplication and verification, such as at border checkpoints. Biometrics are re-enrolled when the NRIC or FIN card is replaced (for example, due to loss or damage). See Box 2.2.2 for more information on the NRIC.

Box 2.2.2 The National Registration Identity Card (NRIC)



The NRIC is a polycarbonate card with several physical security features, such as an alternating of the lion head symbol and the NRIC number when observed from different angles. The NRIC number is included in a barcode on the back, along with an image of the individual's fingerprint. The NRIC for citizens is pink, whereas the NRIC for permanent residents is blue; other types of residents are also differentiated by distinct card designs. The specifications have generally been the same since the 1990s; however, blood type was removed from the card in 2002. There is no expiry date for the NRIC.

On several occasions, the government considered introducing a smartcard as the basis for digital identity. However, after comparing a smartcard vs. an app and considering various factors pertaining to usability and security, the chosen form was an app. Additionally, there was potential to incorporate digital representations of physical cards, as is now seen with the digital IC in Singpass. This reflects the experience in other countries, particularly given the cost and complication of issuing smartcards compared to the utility and ease of use of digital credentials.

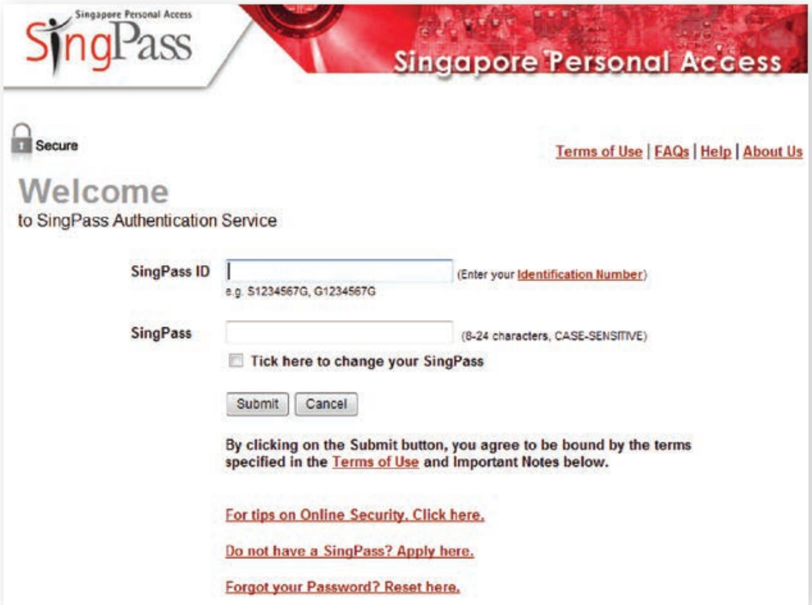
If a citizen applies for a new passport with ICA, the facial image is stored in their NRIC record, which helps with the implementation of Singpass, as a more recent facial image can be used as a reference for Identiface. It is mandatory for citizens to re-enrol their fingerprints and irises at the ages of 30 and 55 if they have not been issued a replacement NRIC within the last 10 years. MOM enrols fingerprints and facial images for work pass holders.

2.3 History and Evolution of Singpass

Singpass began very simply in 2003 as a username and password to act as a single sign-on to government websites (see figure 2.3 for an early screenshot). As evident in the timeline shown in table 2.3, Singpass has undergone a progressive evolution over the past 20 years to become one of the world's leading examples of an NDI platform. GovTech and its predecessors have adapted Singpass to changing user needs, emerging technologies, and external events, such as the passing of the Personal Data Protection Act and a shift in user preferences from desktop/browser-based access to a more mobile-centric means of service.

Examples of this evolution include the introduction of Myinfo for consented data sharing, the expansion to private sector services, the transition to a smartphone application, and the most recent addition of Identiface (facial verification) for stronger identity verification.

Figure 2.3 Example of an Early Singpass Login Screen Showing a Username and Password



Secure

Terms of Use | FAQs | Help | About Us

Welcome
to SingPass Authentication Service

SingPass ID (Enter your Identification Number)
e.g. S1234567G, G1234567G

SingPass (8-24 characters, CASE-SENSITIVE)

□ Tick here to change your SingPass

Submit Cancel

By clicking on the Submit button, you agree to be bound by the terms specified in the Terms of Use and Important Notes below.

For tips on Online Security, Click here.

Do not have a SingPass? Apply here.

Forgot your Password? Reset here.

In terms of development and technological evolution, Singpass began as a completely on-premises solution built by a commercial vendor. It was initially deployed at physical data centres, an approach often referred to by GovTech as the "out-sourced" approach. Today, the majority of the back-end components run on the Government on Commercial Cloud (GCC) and product management; most aspects of development are handled in-house, using supplied components where appropriate—such as for fraud detection and biometric verification.

The Ministry of Finance (MOF), and GovTech formed a committee in the early days of platform design to ensure buy-in and ownership for the target architecture. It was also vital that Singpass solve shared problems—in many agencies it was clear that the same questions were being asked of citizens and residents that had been asked elsewhere in government systems. Introducing Singpass and Myinfo reduced the frustration of having different login credentials and repeat information for both citizens and government agencies. Government agencies benefitted by focusing on their core business rather than running and protecting authentication systems and maintaining personal data securely.

Table 2.3 Timeline of Major Singpass and API Exchange (APEX) Events

Year	Event	Impact
2003	Singpass launches, utilizing username and password for login	Users are able to reliably prove who they are to digital government services for the first time in Singapore.
2014	Two factor authentication (2FA) is introduced	The introduction of 2FA vastly increases the protection of user accounts from password compromise.
2015	Personal Data Protection Act (PDPA) is passed	The PDPA prompts GovTech's predecessor (Infocomm Development Authority of Singapore—IDA) to consider identifying verified information in government, referred to as the 'single source of truth.' This leads to the 'Tell us once' policy, reducing the need for government agencies to hold duplicate personal data about individuals.
2016	Policy splits government and public- facing digital services	Drives the requirement for a bridge or gateway allowing government agencies to share data from intranet to internet-facing services, which serves as the catalyst for the development of APEX as a data sharing framework.
	Myinfo launches	Myinfo begins as a platform to help users to pre-fill digital forms automatically instead of repeatedly for every transaction. To access the platform, users must authenticate using Singpass.
	Corppass launched	A single digital identity for legal entities is established, consolidating various different authentication and authorization platforms.
2017	APEX introduced	APEX is quickly recognized as a significant information infrastructure (SII) due to its enabling role for digital services.
2018	Digital Government Blueprint (DGB) launched	The DGB highlights how national digital identification (NDI) is an enabler for digital government and the broader digital economy.
	Release of Singpass application (October)	The mobile and crypto-based Singpass application is first released, after being announced in 2017.
2020	Launch of Identiface	A higher level of authentication assurance is offered for users and relying parties (RPs).
	Singpass app reaches 1 million users (March)	Significant adoption in less than six months demonstrates the potential value to citizens and residents
2021	Singpass revamps branding and user experience	Implemented due to recognition for the wide range of services provided under Singpass and a result of continuous user research. Myinfo is reframed as a product of Singpass, instead of as a separate platform.
	Application programming interface (API) standards formally introduced	A key opportunity to introduce formal API standards, as plans are developed to extend the use of the API gateway, encompassing the private sector and a move to a cloud-based version of APEX.
	Singpass app reaches 3 million users (August)	The COVID-19 pandemic drives adoption by a factor of three.
2022	Immigration and Checkpoints Authority (ICA) introduces digital birth and death certificates	A key demonstration of how digital technology can enable convenient, yet highly secure, public services.
	First Association of Southeast Asian Nations (ASEAN) digital identity workshop is convened	Organized by the ASEAN Secretariat and Singapore Ministry of Trade and Industry, reflecting the leading role of Singapore in digital government and digital ID.
2023	Cloud version of APEX is due to go live (March)	Increases the ability of APEX to scale and support further digital services.

2.4 Singpass Products and Processes

2.4.1 Account Creation and Recovery

Any Singaporean citizen, permanent resident, or FIN-holder can create a Singpass account using their NRIC number or FIN and demographic information. An individual's NRIC number or FIN can only be connected to one smartphone at any time, and only one NRIC number or FIN can be attached to a Singpass application installation.

There are two main methods of identity verification for the creation and recovery of an account, which are both remote (essentially meaning there is no need to go to a government office):

- **Face verification:** Using the Identiface feature, the user takes a selfie, which is matched against the facial image in the user's NRIC or FIN record. An account is instantly created.
- **PIN mailer:** A one-time password is mailed to the address attached to the user's NRIC or FIN record. This process may take several days, depending on mail delivery.

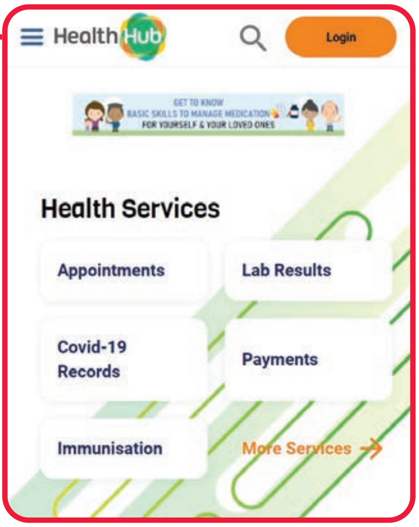
Once the account is created and the user is linked to the device, the user is able to set a password and can provide their email address and/or mobile phone number for future one-time password requests to facilitate authentication.

2.4.2 Login (Authentication)

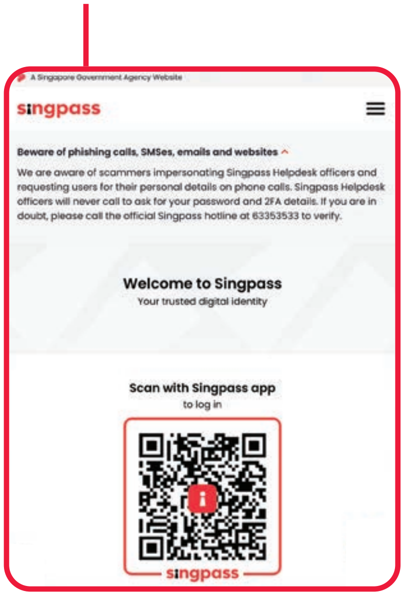
Login is a password-less login method that enables citizens and residents (including on behalf of a legal entity) to easily and securely access public and private sector digital services. This process uses Open ID Connect (OIDC) protocols.

To use Login:

1 The citizen or resident accessing a smartphone application or website will tap or click a link to "Log in" or "Sign in."



2 The relying party's application or website will communicate with the Singpass back-end to direct the user to a Singpass webpage with a unique and time-bound QR code.



A Singapore Government Agency Website

singpass

Beware of phishing calls, SMSes, emails and websites

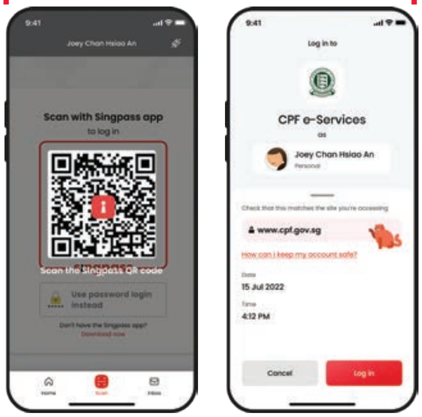
We are aware of scammers impersonating Singpass Helpdesk officers and requesting users for their personal details on phone calls. Singpass Helpdesk officers will never call to ask for your password and 2FA details. If you are in doubt, please call the official Singpass hotline at 63353533 to verify.

Welcome to Singpass
Your trusted digital identity

Scan with Singpass app
to log in

singpass

3 The user scans or taps the QR code, bringing them to the Singpass application. In order to reduce risks of a "man-in-the-middle" attack, information about the relying party and or application website will be displated for the user's confirmation.



9:41

Joey Chan Hsiao An

Scan with Singpass app
to log in

Scan the Singpass QR code

Use password login instead

Don't have the Singpass app?
Download now

9:41

Log in to

CPF e-Services
as

Joey Chan Hsiao An
Personal

Check that this matches the site you're accessing

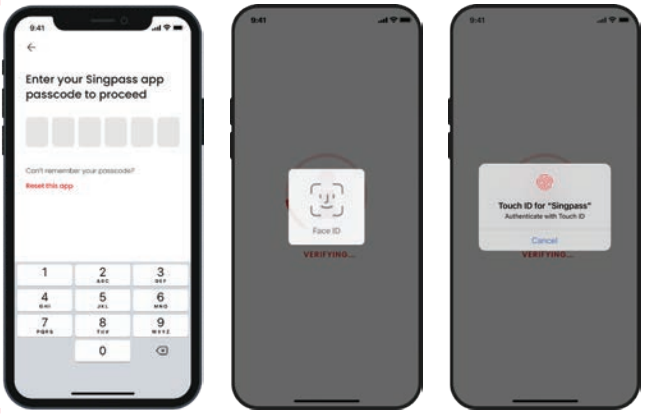
www.cpf.gov.sg

How can I keep my account safe?

Date
15 Jul 2022

Time
4:12 PM

4 If the user responds affirmatively, they will be asked to authenticate themselves inside the Singpass application using either a six-digit PIN (set up inside the application), SMS one-time password, or the smartphone fingerprint or face verification unlock feature.

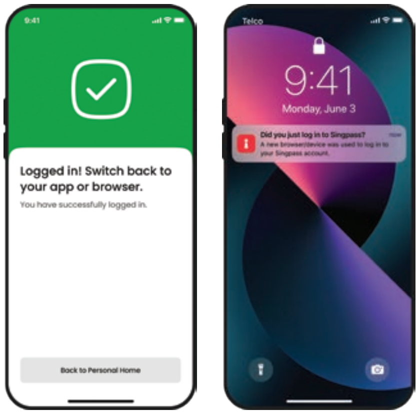


9:41

Enter your Singpass app passcode to proceed

Can't remember your passcode?
Reset this app

5 The Singpass back-end will communicate the authentication result with the relying party's website or smartphone application. The user will also receive a notification of a login transaction occurring.



9:41

Logged in! Switch back to your app or browser.
You have successfully logged in.

Telco

9:41
Monday, June 3

Did you just log in to Singpass? now
A new browser/device was used to log in to your Singpass account.

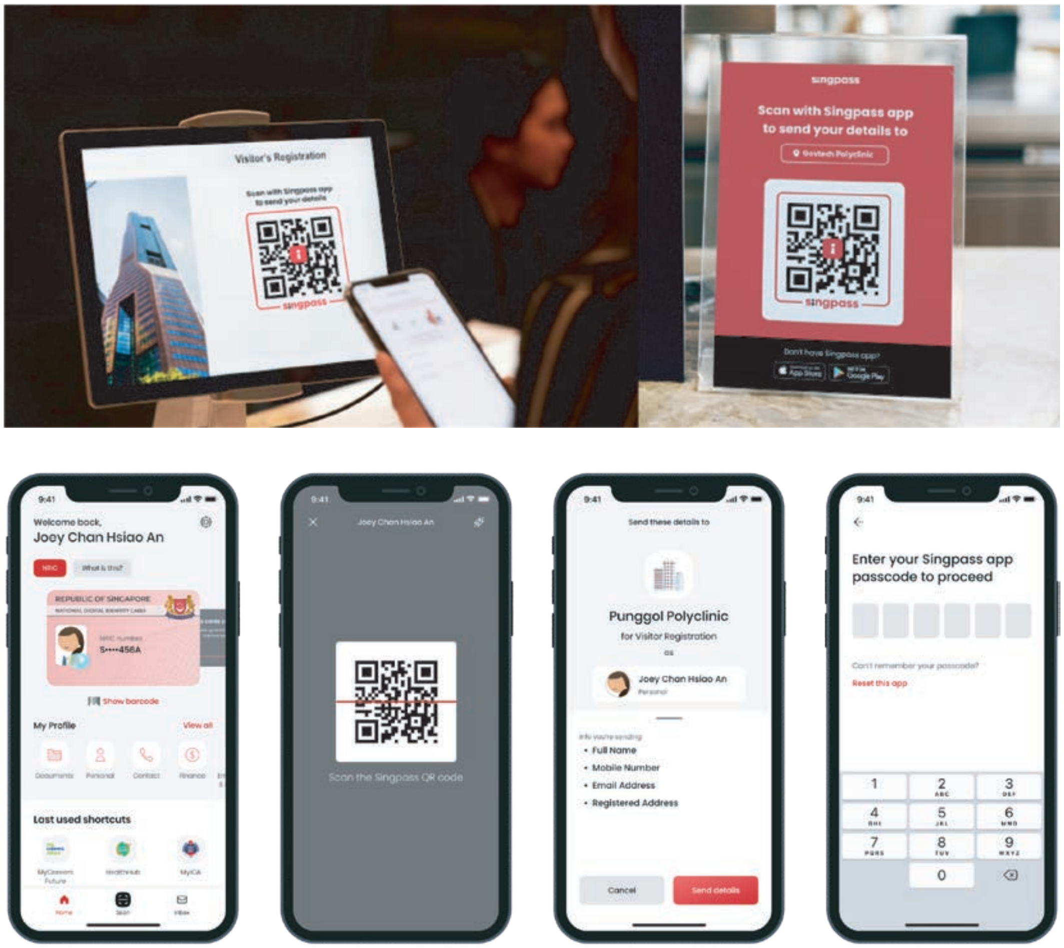
2.4.3 Verify

Verify enables users to perform face-to-face identity verification and secure transfer of personal information through the scanning of QR codes with their Singpass app. This allows users to complete contactless transactions without the need to share physical documents, such as identity documents. It follows a similar process to Login, except that the QR code is static (see figure 2.4.3).

Verify is currently used for new patient registration at polyclinics, age verification when purchasing alcohol at vending machines, and registration for building entry, donations, and car test drives.

SingHealth Polyclinics uses Verify for new patient registration. Compared to traditional registration methods, Verify halved the processing time to register a new patient, from an average of six minutes to three minutes. This reduced crowding at clinic registration counters.

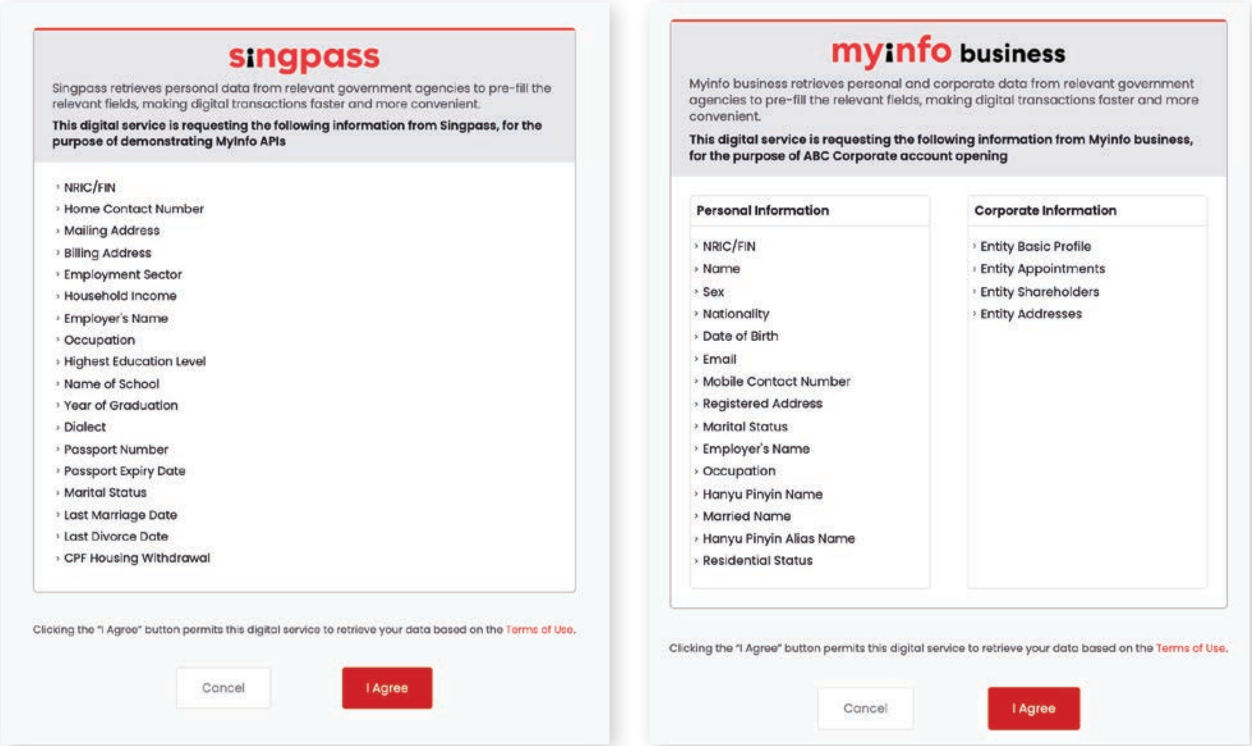
Figure 2.4.3 Verify for Face-to-Face Access to Services



2.4.4 Myinfo

Myinfo enables users to consent to the sharing of their personal data stored in trusted government databases with digital services, as well as to pre-fill digital forms. The process is similar to Login; however, the user is shown additional information about what specific data attributes the relying party is requesting access to, and the purpose of the transaction, before being given the opportunity to provide consent or to cancel the transaction (see figure 2.4.4).

Figure 2.4.4 Examples of Myinfo Individual and Myinfo business Consent Steps



Singpass retrieves personal data from relevant government agencies to pre-fill the relevant fields, making digital transactions faster and more convenient.

This digital service is requesting the following information from Singpass, for the purpose of demonstrating MyInfo APIs

- NRIC/FIN
- Home Contact Number
- Mailing Address
- Billing Address
- Employment Sector
- Household Income
- Employer's Name
- Occupation
- Highest Education Level
- Name of School
- Year of Graduation
- Dialect
- Passport Number
- Passport Expiry Date
- Marital Status
- Last Marriage Date
- Last Divorce Date
- CPF Housing Withdrawal

Clicking the "I Agree" button permits this digital service to retrieve your data based on the Terms of Use.

Myinfo business retrieves personal and corporate data from relevant government agencies to pre-fill the relevant fields, making digital transactions faster and more convenient.

This digital service is requesting the following information from Myinfo business, for the purpose of ABC Corporate account opening

Personal Information

- NRIC/FIN
- Name
- Sex
- Nationality
- Date of Birth
- Email
- Mobile Contact Number
- Registered Address
- Marital Status
- Employer's Name
- Occupation
- Hanyu Pinyin Name
- Married Name
- Hanyu Pinyin Alias Name
- Residential Status

Corporate Information

- Entity Basic Profile
- Entity Appointments
- Entity Shareholders
- Entity Addresses

Clicking the "I Agree" button permits this digital service to retrieve your data based on the Terms of Use.

For Myinfo individual, approximately 150 data attributes from more than 10 government agencies are available for consented data sharing. These range from core demographic information held by ICA and taxation information held by the Inland Revenue Authority of Singapore (IRAS), to employer information held by the Ministry of Manpower (MOM), and vehicle information held by the Land Transport Authority. The exact attributes, the population that they are available to serve (specifically, citizens, permanent residents, and FIN holders), and the source are well-catalogued on the NDI developers' portal.[8]

[8] Singpass API. 2022. "Myinfo API Data." https://api.singpass.gov.sg/library/myinfo/business/implementation-myinfo-data

Myinfo coordinates the gathering of government data via published APIs and the use of APEX acting as an aggregator and an orchestration point for service providers to request multiple data attributes relating to a single person. In this case Myinfo makes onward requests from the relevant API providers in government agencies, then collates the responses into a single response to be sent back to the initiating service.

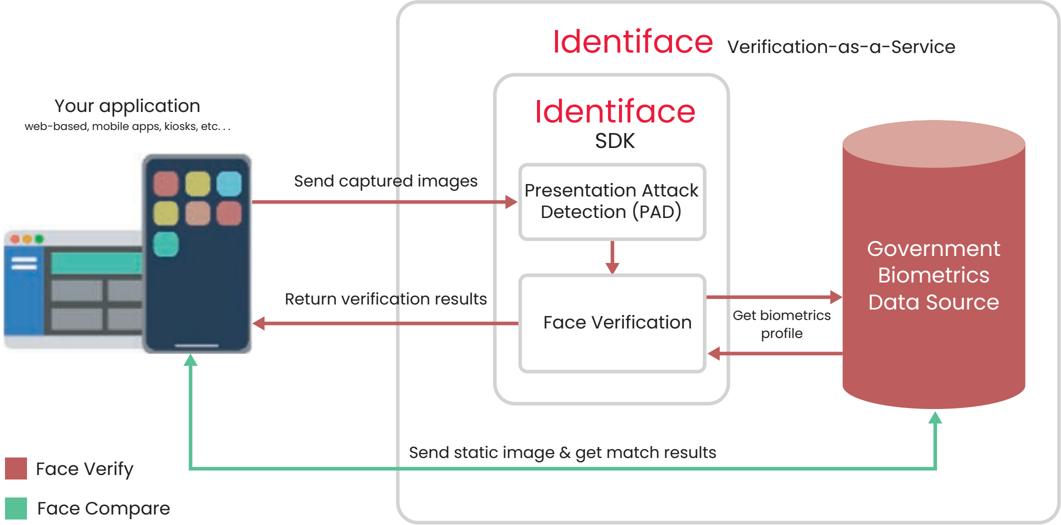
Myinfo removes manual data entry and verification requirements. This results in higher data quality and facilitates "instant" approvals, thereby saving time and increasing efficiency in the process. By retrieving data directly from various government sources, Myinfo enables government agencies and businesses to complete their "Know Your Customer" (KYC) processes without the need for customers to provide additional supporting documents or to access a third party to have the information verified.

2.4.5 Identiface (Face Verification)

Launched in 2020, Identiface is a more advanced method of authentication than Login. Login authenticates the user on the individual's device, whereas Identiface involves the user taking a selfie of their face, which is then compared against the latest facial image provided to the ICA or MOM against their NRIC number or FIN (for example, that of the latest NRIC, work pass, or Singapore passport). It can be integrated into websites—therefore not requiring the user to have a smartphone application—or smartphone applications, as well as face-to-face situations.

Identiface involves two different services, both of which require the NRIC number or FIN. Face Verify embeds liveness detection capabilities into the process, which

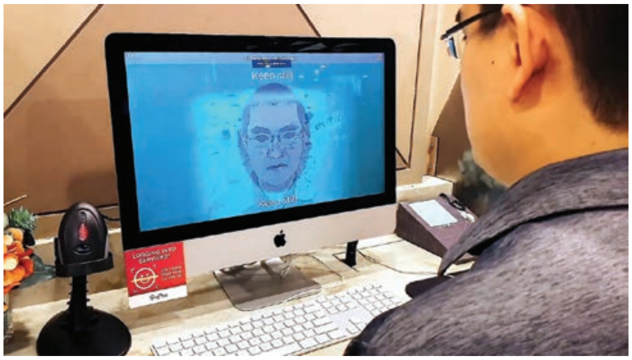
Figure 2.4.5.1 Illustration of the Face Verify and Face Compare Services from the Singpass Developer's Portal


Identiface Verification-as-a-Service
Your application
web-based, mobile apps, kiosks, etc. . .
Send captured images
Return verification results
Identiface SDK
Presentation Attack Detection (PAD)
Face Verification
Get biometrics profile
Government Biometrics Data Source
Send static image & get match results
🟥 Face Verify
🟩 Face Compare

is ideal for unsupervised transactions, to reduce the risks of presentation attacks. In contrast, Face Compare sends a static image for verification. Face Compare can only be used in tandem with Face Verify, given the risks of presentation and injection attacks.

Identiface was introduced to facilitate higher levels of assurance and greater inclusion, essentially because it does not require a user to have a smartphone application and can mitigate the challenges some users may face in remembering PINs and using the Login feature (see example in figure 2.4.5.2). It is also used during the onboarding and account retrieval processes for the Singpass application, as well as an additional, prompted presence-check for fraud prevention if the Singpass back-end detects unusual transactions from a user.

Figure 2.4.5.2 Identiface Used through a Web Browser



Community centers and government offices have been piloting face verification since 2020 with over 81,000 transactions at these kiosks verified through the Identiface API. Users who visit the service centers to reset their Singpass passwords have also seen a reduction in wait time of over 10 minutes.

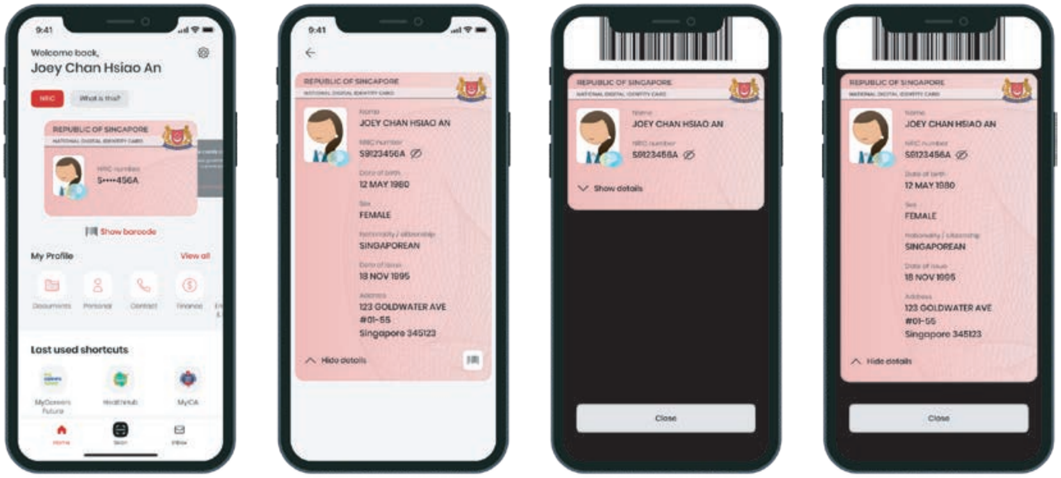
As a privacy-by-design measure, the facial image used for the transaction will only be used for the biometric verification process and will be encrypted and removed from government servers after 30 days, allowing time to audit the transaction if necessary.

2.4.6 Digital Identity Card (IC)

Launched in 2022, the digital IC is digital representation of the user's NRIC or FIN card that can be used in an in-person setting to prove identity. In general, the purpose of the digital IC is to solve the problem of when an individual needs to show a physical card, alleviating the need to carry various cards for physical transactions. Importantly, the intent of the digital IC is focused on identity verification as opposed to data sharing; instead, Verify and Myinfo continue to provide this service, and in a more secure manner.

All government agencies accept the digital IC, and business are also encouraged to do so. Although there are some use cases where the law still specifically requires a physical card, such as registering a marriage and hotel check-ins, the government is in the process of reviewing the legislation to formalize the use of digital ICs for these exceptions.

Figure 2.4.6 The Digital ID Card (IC) for Singaporeans in Various Forms across the Singpass application



The Singpass application provides users with the ability to access the digital IC from the home page (see figure 2.4.6). To open the digital IC, the user must first authenticate themselves. To preserve the privacy of the user, the NRIC number or FIN is masked by default and is only revealed when the user correctly authenticates with the app and chooses to reveal it.

The digital IC includes a barcode, encoding the NRIC number or FIN of the individual, and security features to prevent tampering or screen copying (and subsequent spoofing), including:

- **Profile Photo:** The facial image shown should match the user's face. This is their latest facial image submitted to ICA or MOM.
- **Holographic Logo:** A lion crest overlaid with an animated holographic effect confirms that the digital IC is not a screenshot.
- **Screenshots Disabled:** Screenshots are disabled on Android and iOS; the holographic effect disappears when the screen is being recorded.
- **Quality of Image:** As the detailed background is not simple to reproduce, a spoof of the digital IC may be of poor quality.
- **Interactivity:** Viewers may ask the user to use relevant features, such as re-opening it through the Singpass application homepage, expanding details, and showing the barcode, to prove that it is not a screenshot or video.

As with many GovTech products, the digital IC was designed as a pragmatic and effective approach, leading to solutions that have the highest possible impact without requiring an overly complex, hard-to-deliver technical resolution. The digital IC is more appropriate to most in-person transactions and is seen as convenient to many users. It is also helpful in everyday interactions; for example, if the traffic police need to check an individual's details, they can use the digital driving license, which alleviates the necessity to carry physical documents.

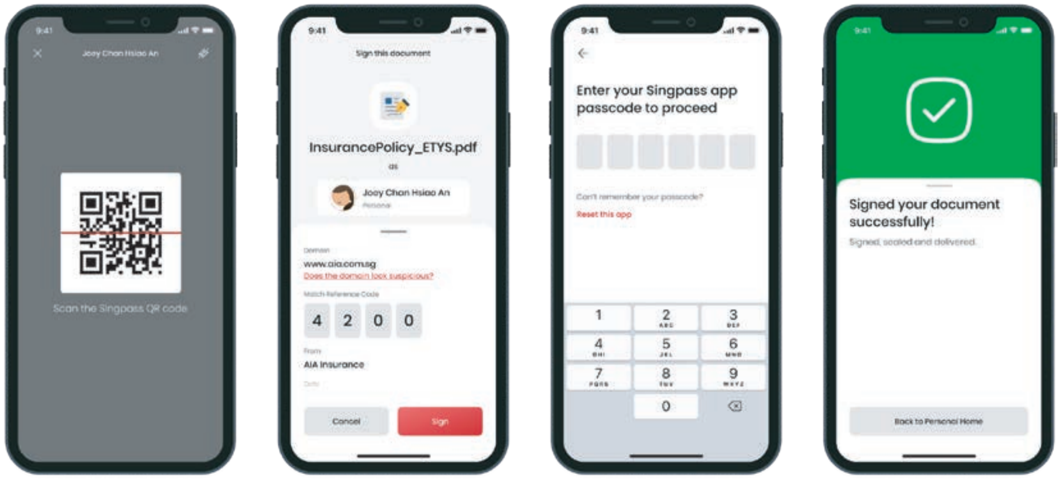
The digital IC is visual, rather than a data representation of the physical card, so it does not follow standards such as those established by the International Organization for Standardization (ISO) for a mobile driving license, or mDL (ISO/IEC 18013-5:2021). From an international point of view, there is currently no provision for cross-border use for credentials such as the driver's licence. Therefore, it is currently low-priority for the digital IC to adopt the ISO/IEC 18013-5:2021 standard.

2.4.7 Sign

The Singpass application facilitates user ability to digitally sign agreements with businesses that are integrated with one of Singpass's digital signing partners. Sign uses signing certificates issued by the National Certification Authority, which means that the signatures will be regarded as secure electronic signatures under Singapore's Electronic Transactions Act.

The process (as shown in figure 2.4.7) is similar to Login. A user taps or scans a unique QR code presented on a web browser and is presented with information about the document they are signing. There is also a four-digit match reference code that should be compared against the four-digit code in the agreement that the user is signing.

Figure 2.4.7 The Sign Process



Scan the Singpass QR code

Sign this document

InsurancePolicy_ETYS.pdf

as

Joey Chan Hsiao An
Personal

Domain
www.aia.com.sg
Does the domain look suspicious?

Match Reference Code
4 2 0 0

From
AIA Insurance

Enter your Singpass app passcode to proceed

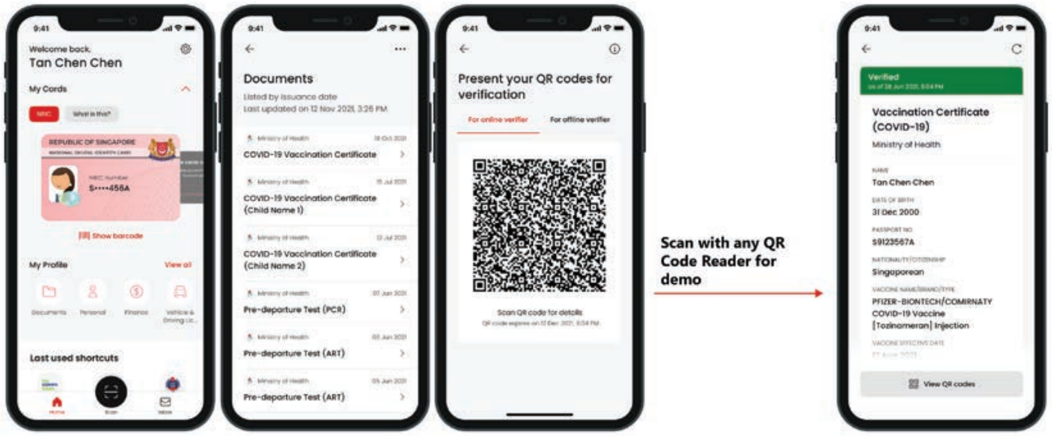
Can't remember your passcode?
Reset this app

Signed your document successfully!
Signed, sealed and delivered.

2.4.8 Document Wallet

In tandem with the launch of the digital IC in 2022, Singpass introduced a digital wallet functionality to provide the ability to store and present digital representations of other government-issued documents. Initial use cases include COVID-19 test results (as shown in figure 2.4.8.1) and vaccination certificates (in the HealthCerts standard format, allowing the QR code to be securely verified anywhere), as well as a digital driving license (DL) similar to the digital IC format. The digital DL (figure 2.4.8.2) is a good example of how GovTech collaborates with other government agencies, in this case with the Home Team Science and Technology Agency (HTX) and the Singapore Police Force (SPF).

Figure 2.4.8.1 A COVID-19 Vaccination Certificate Presented from the Singpass Document Wallet



Welcome back,
Tan Chen Chen

My Cards

REPUBLIC OF SINGAPORE

NRIC number: S••••456A

Documents

Listed by issuance date
Last updated on 12 Nov 2021, 3:26 PM

- Ministry of Health — COVID-19 Vaccination Certificate
- Ministry of Health — COVID-19 Vaccination Certificate (Child Name 1)
- Ministry of Health — COVID-19 Vaccination Certificate (Child Name 2)
- Ministry of Health — Pre-departure Test (PCR)
- Ministry of Health — Pre-departure Test (ART)
- Ministry of Health — Pre-departure Test (ART)

Present your QR codes for verification

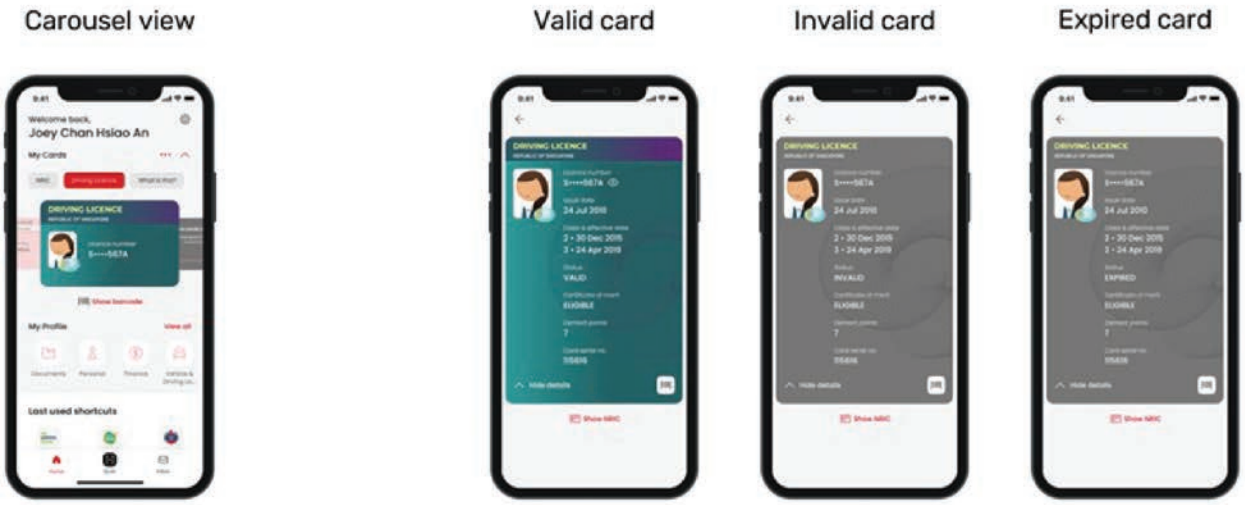
Scan QR code for details

Scan with any QR Code Reader for demo

Vaccination Certificate (COVID-19)
Ministry of Health

NAME: Tan Chen Chen
DATE OF BIRTH: 31 Dec 2000
PASSPORT NO: S9123567A
NATIONALITY/CITIZENSHIP: Singaporean
VACCINE NAME/BRAND/TYPE: PFIZER-BIONTECH/COMIRNATY COVID-19 Vaccine [Tozinameran] Injection
VACCINE EFFECTIVE DATE

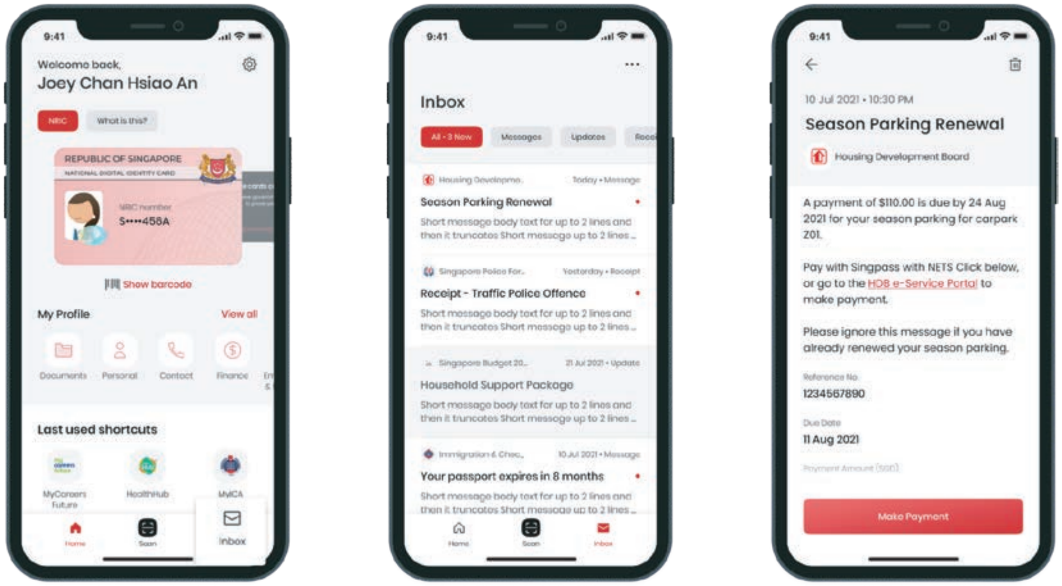
Figure 2.4.8.2 Digital Driving License (DL) Stored in the Singpass Document Wallet in Various States of Validity



2.4.9 Notify

Notify enables Singpass users to receive personalized inbox public announcements; personal reminders; and important messages, such as document updates, directly from government agencies. Current examples (figure 2.4.9) include Singpass transaction notifications, payment reminders, pre-departure COVID-19 test certificate and COVID-19 vaccination certificate notifications, and passport renewal and NRIC re-registration reminders.

Figure 2.4.9 Example of Announcements and Alerts Received through Notify



Housing Developme.. Today • Message
Season Parking Renewal
Short message body text for up to 2 lines and then it truncates Short message up to 2 lines ...

Singapore Police For.. Yesterday • Receipt
Receipt - Traffic Police Offence
Short message body text for up to 2 lines and then it truncates Short message up to 2 lines ...

Singapore Budget 20... 21 Jul 2021 • Update
Household Support Package
Short message body text for up to 2 lines and then it truncates Short message up to 2 lines ...

Immigration & Chec... 10 Jul 2021 • Message
Your passport expires in 8 months
Short message body text for up to 2 lines and then it truncates Short message up to 2 lines ...

10 Jul 2021 • 10:30 PM
Season Parking Renewal
Housing Development Board

A payment of $110.00 is due by 24 Aug 2021 for your season parking for carpark Z01.

Pay with Singpass with NETS Click below, or go to the HDB e-Service Portal to make payment.

Please ignore this message if you have already renewed your season parking.

Reference No.
1234567890

Due Date
11 Aug 2021

Payment Amount (SGD)

2.4.10 Corppass and Myinfo business – A Digital Identity for Legal Entities

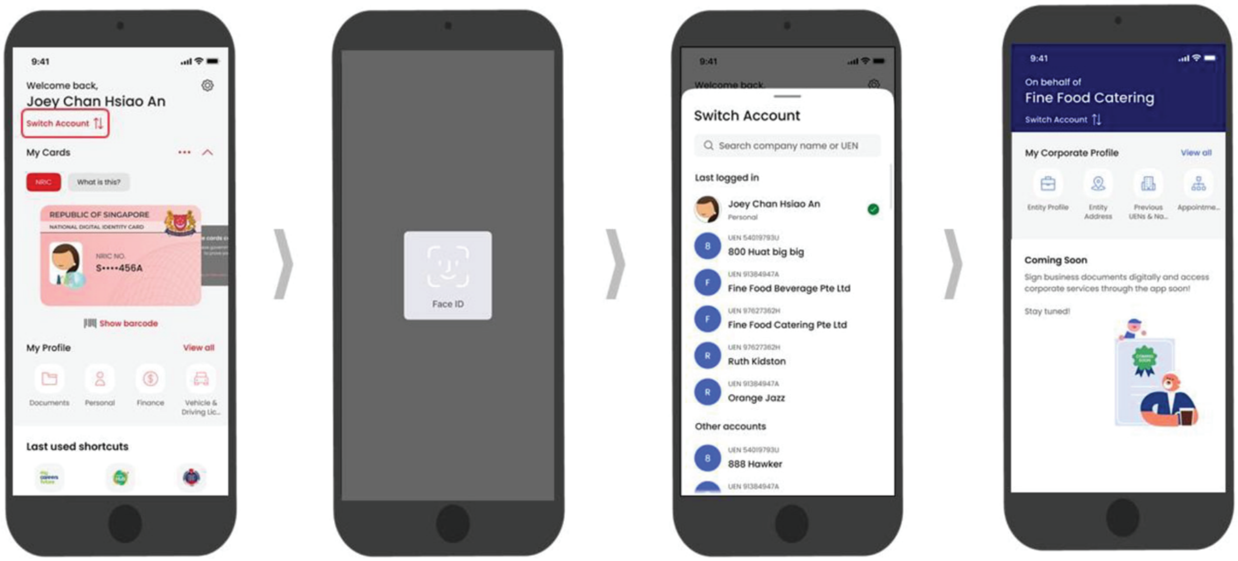
Corppass was launched by IDA in 2016 as a new corporate digital identity for businesses and other legal entities, such as non-profit organizations and associations, to access government digital services—for example, filing taxes or applying for permits and licenses.

As the name suggests, Corppass initially drew on the experience of Singpass, and authentication comprised a username and password. Businesses and legal entities with a local Unique Entity Number (UEN) could identify registered officers, such as owners, directors, and corporate secretaries, as well as Corppass administrators (appointed by registered officers to manage Corppass accounts).

Prior to the launch of Corppass, businesses and other legal entities used either Singpass or the E-Services Authorisation System (EASY), depending on which government agency they were transacting with. The introduction of Corppass reflected feedback from the business community that Singpass should only be used for personal transactions, due to privacy concerns. For example, employees often shared their Singpass username and password with colleagues when they went on leave, in order to ensure that transactions could still be undertaken.

In 2021, Corppass accounts and authentication evolved to become a feature in Singpass for local business and other entities. Registered officers can now change between personal and Corppass profiles within the Singpass application, which differentiates the look and feel for Corppass profiles from a personal profile (figure 2.4.10). Corppass administrators still use the Corppass website to manage accounts, signing in using their personal Singpass. Foreign entities without a UEN, including those that must file tax returns, also use the previous Corppass username and password system, but with the added layer of 2FA.

Figure 2.4.10 Corppass Profile in the Singpass application



Sign business documents digitally and access corporate services through the app soon!

Stay tuned!

2.5 Key Enablers

2.5.1 Legal Framework

Specific legislation for NDI has not been required to date. Several underlying laws are in place that create a legislative framework through which Singpass can be reliably used in Singapore. These key legislative acts are as follows:

- **The Public Sector (Governance) Act:** This law governs, among other topics, the management of data by government agencies, including personal data protection and data sharing. It is complemented by the Instruction Manual for Infocomm Technology and Smart Systems Management, which provides WOG policies, standards and guidance on good practices related to data classification, data protection and security, data acquisition, data processing and fusion, and data access and distribution.
- **The Personal Data Protection Act:** This law provides a baseline standard of protection for personal data by the private sector in Singapore. It complements sector-specific legislative and regulatory frameworks, such as the Banking Act and Insurance Act. It also comprises various requirements governing the collection, use, disclosure, and care of personal data in Singapore—which is of vital importance to both privacy and trust in a digital identity ecosystem.
- **The National Registration Act:** This law enables Singapore to retain a high-quality, high-coverage foundational ID system upon which Singpass is reliant.
- **The Electronic Transactions Act:** This law is a key legal basis for Singpass by establishing trusted certification authority services in Singapore. Further, it focuses on the facilitation of electronic transactions through the recognition of electronic signatures and records. In an amendment to the law in 2021, Singapore became, the second country to adopt the United Nations Commission on International Trade Law (UNCITRAL) Model Law on Electronic Transferable Records (MLETR) into domestic legislation, a move which sees electronic trade documents, such as promissory notes and electronic bills of lading (eBLs), given the same legal standing as their paper-based counterparts. This move toward further equivalence for electronic records adds opportunities for the use of Singpass to facilitate additional use cases in the private sector.

2.5.2 Technology

2.5.2.1 Architecture and Components

Figure 2.5.2.1 shows the core components of the Singpass architecture and how users interact with it to create a digital identity as part of Singpass and to subsequently use key services, such as Myinfo, to share data with relying party services once authenticated.

More information about the architecture of Singpass is available at: https://api.singpass.gov.sg/library/login/developers/overview-at-a-glance

Figure 2.5.2.1 National Digital Identity (NDI) High-level Architecture

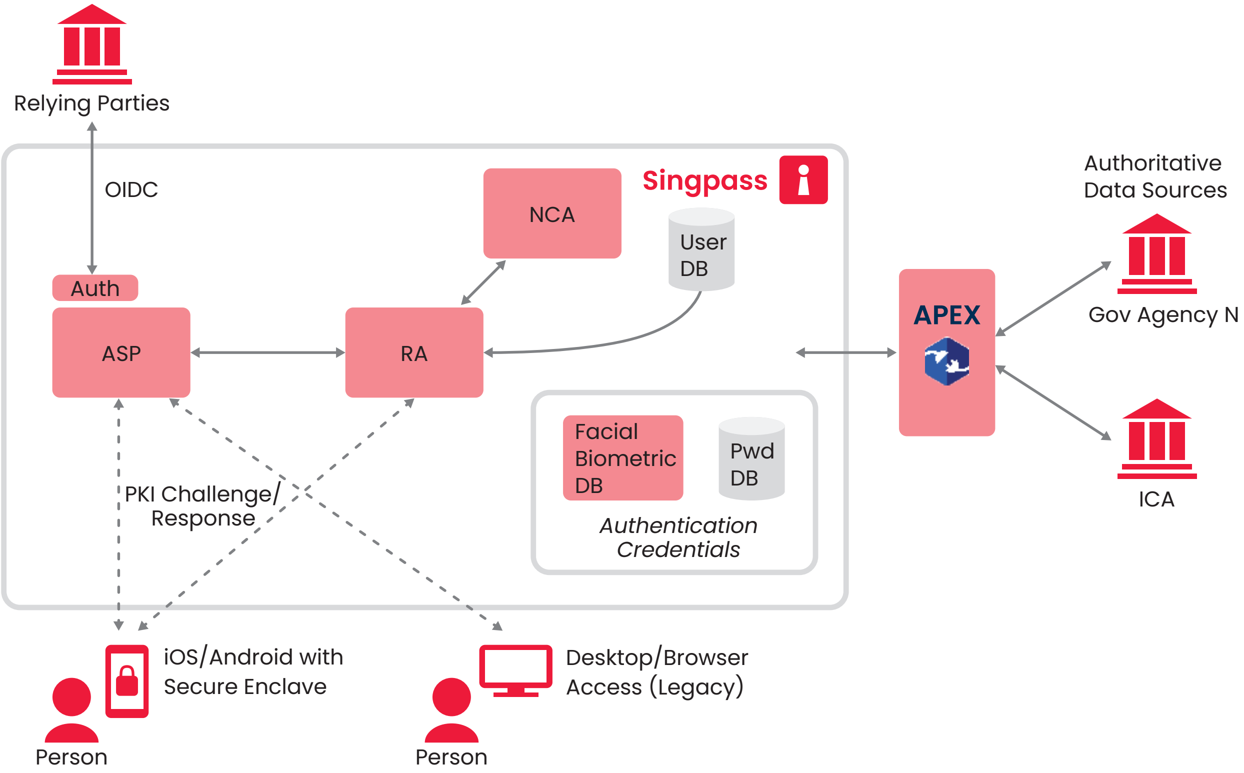


Table 2.5.2.1 National Digital Identity (NDI) High-Level Architecture Definitions

APEX	A secure application programming interface (API) gateway for exchanging data with government databases.
ASP	Authentication Service Provider – Responsible for authenticating existing users (using OpenID Connect—OIDC).
Authentication Credentials	Databases of facial images and passwords for registered Singpass users used during authentication.
NCA	The National Certificate Authority (NCA) is responsible for issuing user certificates that tie a user's public key infrastructure (PKI) credentials to the user's digital identity.
RA	Registration Authority – Acts as an intermediary for verifying requests for a digital certificate. The RA informs the National Certificate Authority (NCA) to issue a certificate and also communicates revocation of digital certificates.
User DB	A database containing the information of all citizens and residents over the age of 15, regardless of their registration status with Singpass. This is used as a reference point during onboarding and is derived automatically from the Immigration and Checkpoints Authority (ICA), a foundational ID system, and the Ministry of Manpower (MOM) data, which issues work passes.

2.5.2.2 *Public Key Infrastructure and Establishing Trust During Onboarding and Use*

A key design decision was to base the trust of a user's Singpass identity on public key infrastructure (PKI), which is also a foundation for other Singpass services, such as Sign. Singpass relies on the National Certificate Authority (NCA) for the issuance and management of digital certificates.

For iOS and Android users, the Singpass onboarding process includes the generation of a secure user PKI keypair in the smartphone's secure enclave. The Singpass application relies upon digital certificates to certify the ownership of credentials, such as a user's identity credential. This means that only the user has ownership of their private key, ensuring that relying parties can trust communication between the smartphone and Singpass services.

Two types of digital certificates are stored on the smartphone:

- **Authentication Certificate:** Used for Login and related products. When users authenticate themselves with Singpass, the authentication certificate is checked for the verification of the user's identity.
- **Signing Certificate:** Used for Sign and Authorize. When an individual uses Sign with Singpass to digitally sign documents, the signing certificate generates a digital signature on the electronic document. This digital signature is cryptographically linked to the signer and can be verified using the signer's public key.

GovTech does not have specific hardware requirements for the smartphone device, but at the point of account creation, the application detects the capabilities of the device with regard to a secure enclave, and if this is present, the onboarding can continue.

The Myinfo service APIs are not accessed directly by the Singpass application and are able to utilize a wider range of public key options from commercial providers, such as Entrust, GlobalSign, VeriSign, and others as described in Myinfo documentation.[9] The core requirement is a X.509 certificate enabling implementation of RSA SHA-256 (as specified in the technical documentation). Furthermore, in terms of the integrity of demographic information, the Singpass back-end utilizes the APEX gateway to pull authoritative data directly from government databases on-demand for onboarding, as well as Myinfo.

[9] For Myinfo documentation and implementation requirements, see:https://api.singpass.gov.sg/library/myinfo/developers/implementation-technical-requirements

2.5.2.3 Authentication Process

Two forms of two factor authentication (2FA) were added to Singpass in 2014: an SMS one-time passcode sent to the user's registered mobile phone number, and a hardware token optionally provided to users who did not wish to use a mobile phone number or were unable to use one. These hardware tokens were issued free of charge but are being retired due to the high cost and increasingly marginal use.

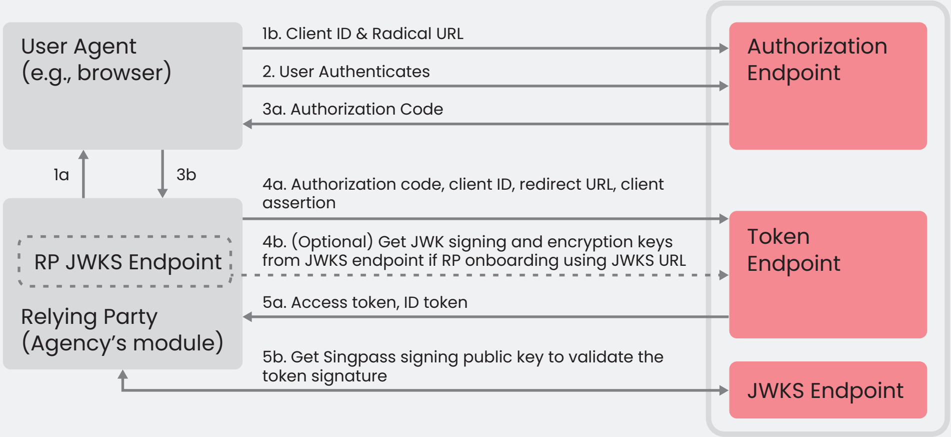
Today's Singpass authentication usually occurs by scanning (in the case of accessing a service through a second device, such as a computer) or tapping (in the case of accessing a service using the smartphone that the application is installed on) a QR code, which serves as an instruction to the Singpass application to start an authentication transaction and includes a unique value representing the specific authentication request from the relying party.

To prove that the user is who they say they are, the Singpass app uses the private key held in the phone's secure enclave to sign the request and send it back to the relying party (at a fixed endpoint for the relying party via the Singpass service) as a response message. Subsequent communication between the application and the relying party currently utilizes OpenID Connect as a protocol. Box 2.5.2.3 explains the process in more detail.

The key advantage for the user is a secure, password-less login that is more convenient to use. For relying parties, there is greater authentication assurance and, particularly for those that are accessed infrequently, allowing users to log in with a mechanism that they are familiar with elsewhere, such as Singpass, reduces issues with account management—that is, forgotten credentials, among others.

Box 2.5.2.3 Technical Authentication Flow for Singpass

Figure B2.5.2.3.1 Singpass Login Flow (OpenID Connect)


User Agent (e.g., browser)
1b. Client ID & Radical URL
2. User Authenticates
3a. Authorization Code
Authorization Endpoint
1a
3b
4a. Authorization code, client ID, redirect URL, client assertion
RP JWKS Endpoint
4b. (Optional) Get JWK signing and encryption keys from JWKS endpoint if RP onboarding using JWKS URL
Token Endpoint
5a. Access token, ID token
Relying Party (Agency's module)
5b. Get Singpass signing public key to validate the token signature
JWKS Endpoint

The technical authentication flow for Singpass (as shown in figure B2.5.2.3.1) comprises the following steps:

Step 1: The relying party requests that the user authenticate.

(a) The relying party sends an authentication request to the Singpass OpenID Provider (OP) to authenticate the end user via user agent.

(b) The request must include the relying party's identity (client ID), redirect uniform resource identifier (URI), and the OpenID scope.

Step 2: Singpass OP will authenticate the end user using one of the available methods.

Step 3: Once the user has authenticated, Singpass issues an authorization code.

(a) Once the end user has been authenticated, Singpass will generate an authorization code.

(b) An authorization code will be redirected to the relying party's server component via user agent. In addition, the authenticated session of the end user is maintained on the user agent and Singpass back-end.

Step 4: The relying party uses the authorization code to request the ID token.

(a) The relying party's server component contacts the token endpoint with authorization code, client identifier, client assertion JSON web token (JWT) and redirect URI.

(b) If the relying party has a JSON web key set (JWKS) endpoint, the Singpass OP will retrieve the encryption and signing keys from this endpoint.

Step 5: Singpass validates the client credential.

(a) Singpass will validate the client credential, authorization code and return ID token, and access token via out-of-band channel.

(b) The relying party can fetch Singpass's signing key via JWKS URL to validate the token's signature.

Note: Singpass is continuously improving. For the latest technical information, including on the authentication flow, please visit the Singpass website: https://www.singpass.gov.sg/.

2.5.2.4 Cloud Adoption

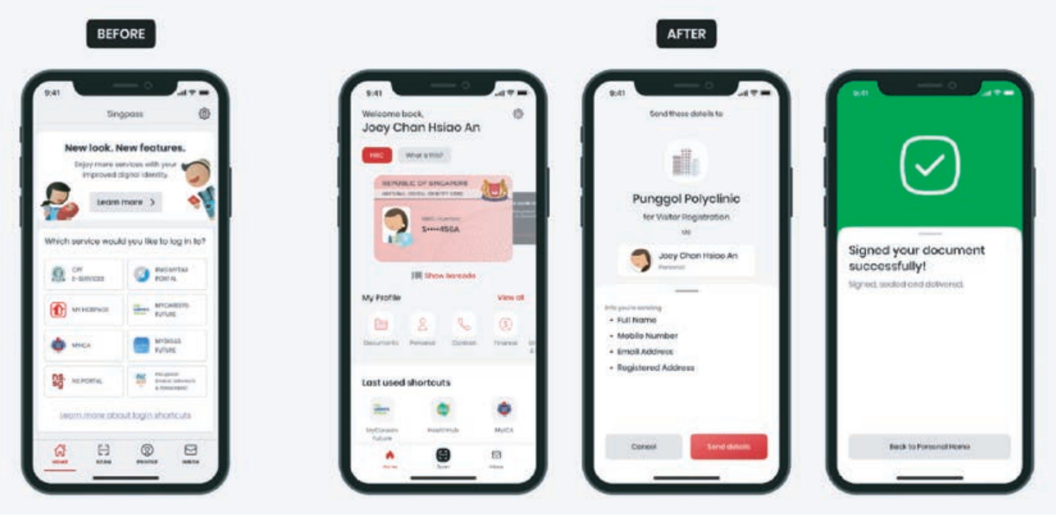
Cloud, through the Government on Commercial Cloud, is now being adopted in a measured approach by the back-end architecture that supports Singpass. This is being implemented where the advantages of cloud can be harnessed to meet the increased demand from both users and relying parties building new products and services. However, in cases where data security is paramount, some services remain under the control of GovTech.

2.5.2.5 User Experience

GovTech and its predecessors have paid significant attention to prioritizing and understanding the needs of users and relying parties for all of their products and services. This includes studying in detail how users interact with Singpass and, as new products and features are added, carrying out user testing and focus group discussions. For example, GovTech has set up Tech Kaki, an open community for citizen participation in the design process,[10] allowing members to obtain first access to new products before they go live, as well as to collaborate with GovTech's development teams. As a result, GovTech is able to analyze the user experience of citizens and residents—and identify where it could be improved.

Most recently, in 2021, several design changes were made to the Singpass application and branding, both in recognition that Singpass had become more than just a login to public and private sector services, and to highlight its full potential to users. More information about this redesign is available at: **https://medium.com/ndi-sg/not-just-for-logging-in-redesigning-singapores-digital-identity-app-545c08d820bb**

Figure 2.5.2.5.1 The Singpass app Before and After Redesign

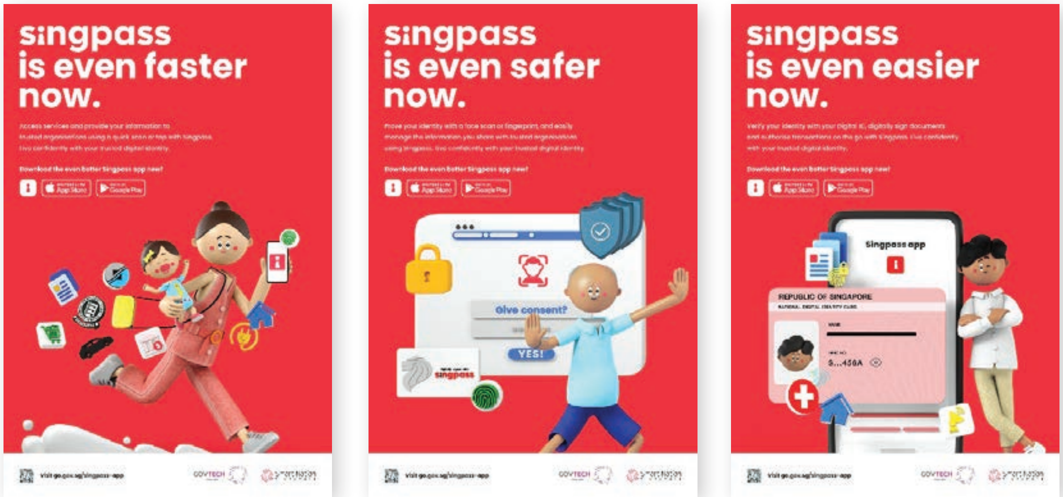


[10] For more information about Tech Kaki, see: https://www.tech.gov.sg/products-and-services/tech-kaki-community/

The look and feel of Singpass was refreshed (figure 2.5.2.5.1), modernizing the brand and building on the strong reputation and trust built over the previous 18 years, aiming to give it a professional yet fresh personality. A unique logo was created, with a lowercase "i" taking the shape of both a human silhouette and a keyhole, to signify a focus on user-centric services and security. Elements of the old Singpass logo, such as the logomark of the "i," were retained to ensure familiarity and build on its established branding. Animated characters and elements that mirrored the landscape and demographics of Singapore were also added.

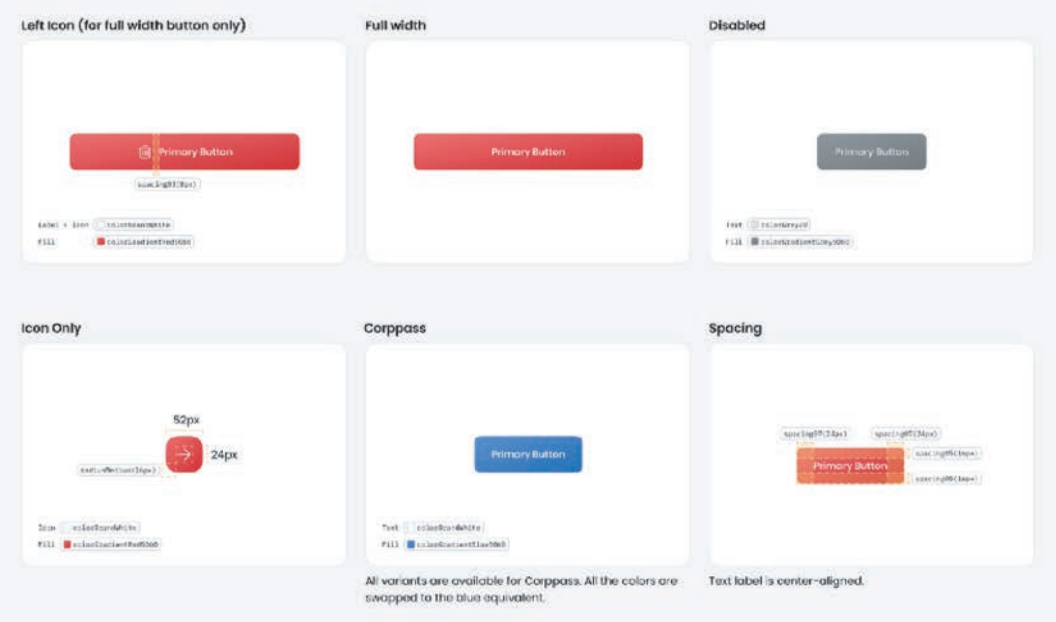
GovTech also introduced new taglines such as, "Even Better," "Even Easier," "Even Safer," "Even Faster," to communicate the attributes that users value in Singpass: convenience, ease of use, and security (figure 2.5.2.5.2). To emphasize Singpass as a user-centric, business-friendly, and inclusive platform, the Singpass website and app were given a visual overhaul.

Figure 2.5.2.5.2 Advertisements Promoting the Refreshed Singpass Brand


singpass is even faster now.
Download the even better Singpass app now!
singpass is even safer now.
Give consent?
YES!
Download the even better Singpass app now!
singpass is even easier now.
Singpass app
REPUBLIC OF SINGAPORE
Download the even better Singpass app now!

Nevertheless, it was not just how the application looked that was important; GovTech sought to address how it was used. In many cases, this meant striking a balance between convenience and security when designing the new user interface. To support developers and the wide array of functionalities now seen in Singpass, a more flexible and scalable design system was also developed to ensure that it was easy for developers of relying parties to build new functionalities while maintaining a consistent user experience (figure 2.5.2.5.3; box 2.5.2.5).

Figure 2.5.2.5.3 Examples of Buttons from the New Design System



All variants are available for Corppass. All the colors are swapped to the blue equivalent.

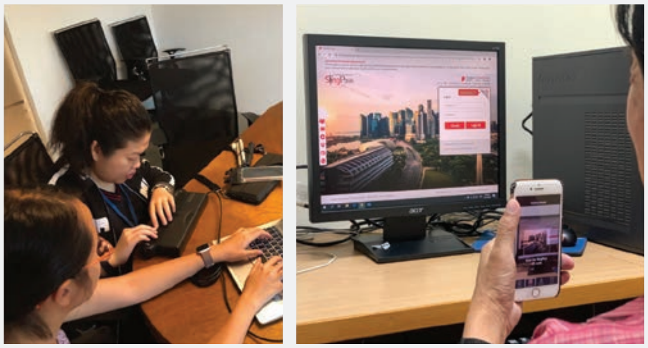
Text label is center-aligned.

Box 2.5.2.5 Designing for Accessibility

Inclusive Design Processes

As part of the process leading up to the 2021 refresh, GovTech designers also began to look at how they could make Singpass more inclusive. Part of this effort was to address the needs of people less able or those with differing needs when accessing technology. This could be due to any number of factors, including physical or sensory disabilities, specific emotional needs, and those with cognitive issues. These considerations do not only make for a more inclusive service, but they usually result in a better experience for all users.

Figure B2.5.2.5.1 Working with Visually Impaired Users during Accessibility Testing



As work began with a research project focusing on the needs of underserved communities, such as persons with disabilities, single mothers, and the elderly, insights from these user testing sessions began to shape the app's development and led to guiding principles such as: "*Be succinct. Provide just enough information for the user to proceed at every step of the user journey.*" For example, catering to native screen reader technologies has become part of the app development process.

(continues)

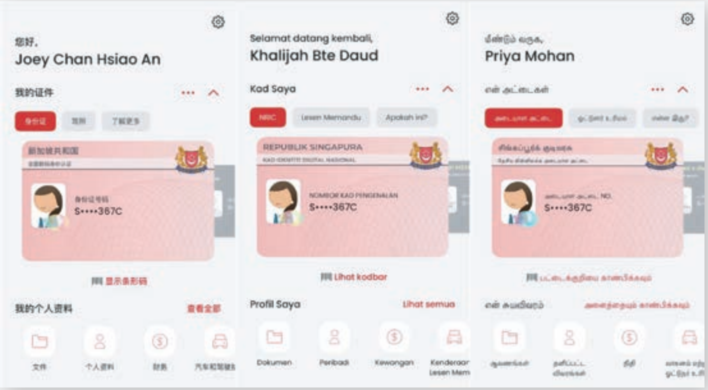
Box 2.5.2.5 Designing for Accessibility *(continued)*

Another key learning point for the research team was that in addition to making Singpass more functionally accessible, the application should empower people with a sense of agency and independence. These key insights have led the Singpass app to become a pleasure to use, and to drive the app to become a much more inclusive service for Singaporeans and residents. This can be observed through the Singpass app reviews, which has a rating of 4.7 on both the Google Play Store and the Apple App Store as of August 2022.

Multi-Language Support

Singapore is a multilingual society with four official languages: English, Chinese, Malay, and Tamil. From an inclusivity point of view, as 11 percent of Singpass app users already set their phones to a language other than English, having Singpass in the four official languages can only be a benefit.

Figure B2.5.2.5.2 One Singpass, Multiple Languages



To address this need, the Singpass app team, assisted by GovTech's Government Digital Services (GDS) division, translated approximately 60,000 words from the existing English version of the Singpass application into each of the other three official languages. But simply translating the text was only one aspect—time was taken to ensure that the translations made sense in each of the languages, and that the same level of readability and understanding was maintained, regardless of which language the user chose.

Translating an app from one language to another has many challenges. For example, words may take up more space than in other languages; therefore, pages might need to be redesigned. Extensive testing of the application has ensured that all users have a consistent experience regardless of language choice. Technical testing was conducted, followed by user testing with Citizen Translators—native speakers/writers who have volunteered with the National Translation Committee (NTC) under the Ministry of Communication and Information (MCI)—to review translated materials.

The fresh eyes of the Citizen Translators allowed them to provide valuable feedback on the translations. This made the difference between a readable app and a truly great experience for native speakers. For example, the English version of the app has a "What is this?" button where users can find out more about the "My Cards" section, which holds users' digital identity cards(ICs). The initial Chinese translation was "这是什么?", a factually accurate but literal translation. However, the Citizen Translators recommended "了解更多," (Chinese for "Understand more") instead, which is fluent and easier to understand for the Mandarin-speaking community.

2.5.2.6 Security

As with almost every official digital system, phishing scams are a problem. GovTech and the Singapore Police Force work closely together to share intelligence of the threat landscape and act accordingly to reduce the risk for Singaporeans and residents. When phishing sites are identified, they can be blocked immediately, and users are informed in case they have been subject to scams.

Monitoring of the underlying infrastructure and applications is implemented to prevent unauthorized use and potential malware attacks, as well as to identify potential issues with the operational capability of Singpass. This includes any particular protection as data passes through the APEX gateway from government APIs to and from internet-facing services.

Fraud analytics is employed to identify and flag unusual activities in real-time, alerting users instantly when unusual activities are detected (e.g., if a Singpass login is performed on a new Internet browser or device, or if the country locations of the Singpass app and the device logging in do not match).

If an individual loses their device, they can deactivate the Singpass app via the Singpass portal using alternative 2FA methods such as Identiface or SMS OTP. The app will prevent the user from using the app if it detects altered setting on the device that could compromised the account. In these cases, the individual will have to either reverse the changes made or set up an account on a different device.

Please refer to the Singpass security page for latest information on the security measures: **https://www.singpass.gov.sg/main/security/?show=use-securely**

2.5.2.7 Data protection and privacy

From a user perspective, when a service requests data, it does so through Myinfo, which means that the data subject is requested to consent to the use of data and is aware of what type of data will be shared.

Myinfo currently only supplies one-time access to data, in the context of a single digital transaction; it does not offer continuous access to data or authorization for an organization to access data multiple times without additional consent. This is seen as better for the user, as it means that consent is sought every time an organization needs to process data, and that the user does not have to remember what they allowed to happen with their data, which, in a digital economy, could be extensive and range across multiple service providers and agencies.

Services wishing to access government data through Myinfo APIs must also complete an application process, during which the need for data is reviewed, and only services where appropriate access to data is demonstrated will be allowed.

Individuals can also access an audit trail of where they have consented to data being used, but this is limited to the use of data for digital transactions in which the user is an integral part of the process flow.

2.5.3 Go-to-Market

2.5.3.1 Support for Citizens and Residents

GovTech has a help desk that handles issues with Singpass and related products for individual users. For issues beyond GovTech's direct control, such as the accuracy of Myinfo data, GovTech coordinates the resolution of these issues or refers users to the appropriate government agency.

If citizens and residents face any problems, including with onboarding and account recovery, they may visit one of 50 Community Clubs (half of all Community Club locations) that also serve as Singpass counters. There, the user can be served face-to-face by Community Club staff to create or recover an account. Community Clubs are well-located and physically-accessible public locations where people gather for group activities, social support, public information, and other purposes. For example, many served as vaccination centers and distribution points for masks during the COVID-19 pandemic.

2.5.3.2 Building Communities, Publishing Documentation, and Onboarding Relying Parties

GovTech places a strong emphasis on community development to build a vibrant developer ecosystem around its products and services. As stated on the GovTech Community Development website, "*We believe that our goal—to build better products for the public good—can be achieved only through meaningful collaboration with the developer community*."[11]

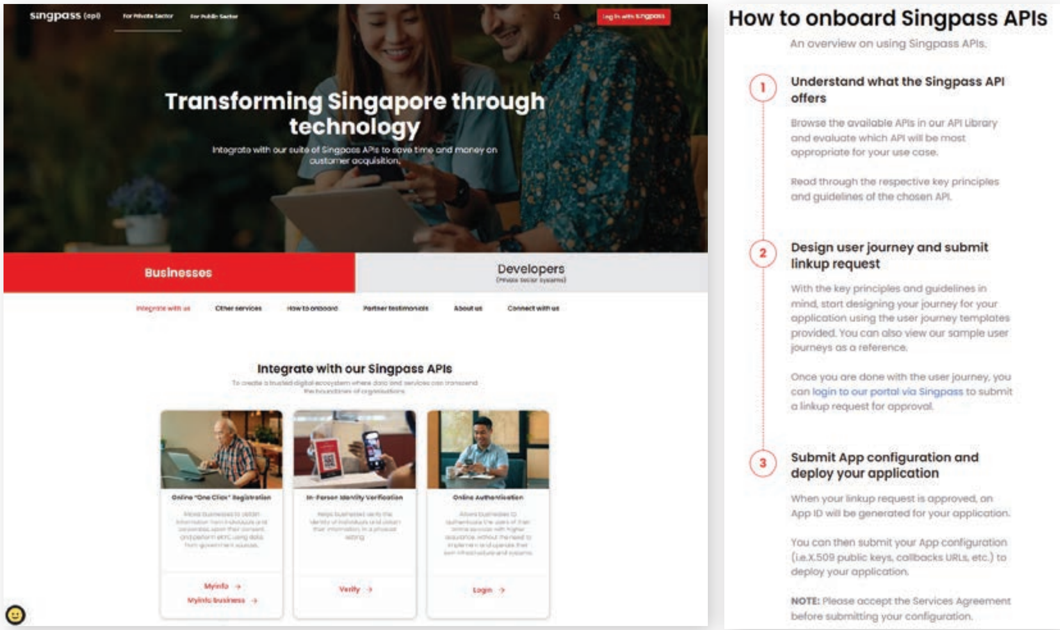
To put this into practice, aside from detailed documentation, guidelines, tutorials, and explanations, Singpass provides developers and partners in government, as well as the private sector, with a self-service developer portal and application process for integration with Singpass APIs.[12] The portal is easy to use and focuses not only on technological integration, but also on walking relying parties through designing new user journeys for their products and services, as enabled by Singpass. For example, the portal contains separate Business and Developer sections, catering to non-technical and technical audiences, respectively.

These resources are accessible without the need of any login to the Singpass API website, in order to encourage interested parties to explore and find out more about Singpass APIs, including key principles, standards, processes, requirements,

[11] For more information about GovTech's Community Development efforts, see: https://www.developer.tech.gov.sg/communities/overview

[12] For more information about the Singpass self-service developer portal, see: https://api.singpass.gov.sg/

Figure 2.5.3.2 The Singpass API Developer Portal and Three-Step Process for Onboarding



singpass (api) For Private Sector For Public Sector Log in with Singpass

Transforming Singapore through technology

Integrate with our suite of Singpass APIs to save time and money on customer acquisition.

Businesses | Developers (Private Sector Systems)

Integrate with us · Other services · How to onboard · Partner testimonials · About us · Connect with us

Integrate with our Singpass APIs

To create a trusted digital ecosystem where data and services can transcend the boundaries of organisations

Online "One Click" Registration
Allows businesses to obtain information from individuals and corporates upon their consent, and perform eKYC using data from government sources.
Myinfo →
Myinfo business →

In-Person Identity Verification
Helps businesses verify the identity of individuals and obtain their information in a physical setting.
Verify →

Online Authentication
Allows businesses to authenticate the users of their online services with higher assurance, without the need to implement and operate their own infrastructure and systems.
Login →

How to onboard Singpass APIs

An overview on using Singpass APIs.

1 **Understand what the Singpass API offers**

Browse the available APIs in our API Library and evaluate which API will be most appropriate for your use case.

Read through the respective key principles and guidelines of the chosen API.

2 **Design user journey and submit linkup request**

With the key principles and guidelines in mind, start designing your journey for your application using the user journey templates provided. You can also view our sample user journeys as a reference.

Once you are done with the user journey, you can login to our portal via Singpass to submit a linkup request for approval.

3 **Submit App configuration and deploy your application**

When your linkup request is approved, an App ID will be generated for your application.

You can then submit your App configuration (i.e.X.509 public keys, callbacks URLs, etc.) to deploy your application.

NOTE: Please accept the Services Agreement before submitting your configuration.

and frequently asked questions. When potential relying parties want to integrate with Singpass and onboard with any of the APIs, the application process begins by logging in using Singpass on behalf of the legal entity, then submitting a proposed user journey and a linkup request for approval.

The portal supports a guided application process for public and private sector relying parties. In conjunction with the application process, there is a range of documentation and a "sandbox" for relying parties to test their new service. While the application process is largely automated, new relying parties are made aware of the need to review their user journeys and re-engineer where necessary, as Singpass and its products, such as Myinfo, will streamline the business process.

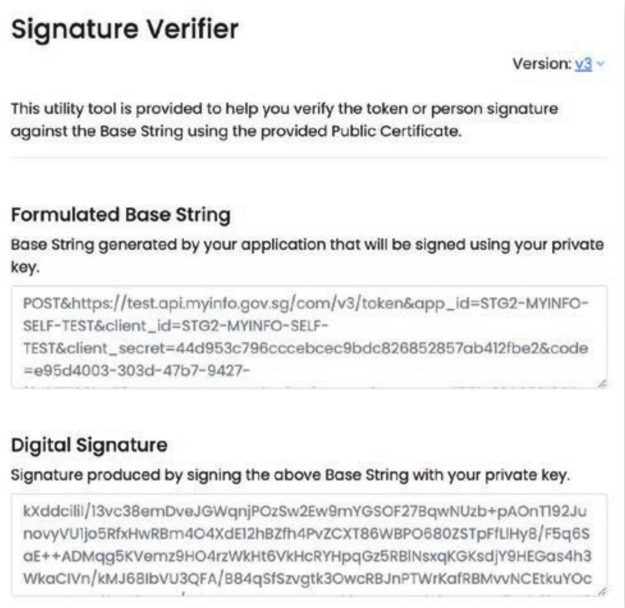
For private sector relying parties, a review process is in place to ensure that the request for data is reasonable. For example, if a bank wants to ask for a customer's address, income statement, etc., that is considered reasonable. However, if the bank asked for unrelated data, then that would not be deemed reasonable. Oversight for this approval is provided through the Smart Nation and Digital Government Office (SNDGO) and GovTech. Once approved, the relying party can then proceed to integrate Singpass API with their user journey that requests data, which is subsequently consented to by the customer or citizen.

More generally, GovTech organizes regular developer events, including its STACK flagship conference and regular STACK-X Meetups. An additional, highly informative resource is the Singapore Government Developer Portal,[13] a one-stop resource hub for government digital products and services. It provides digital government resources, guidelines for project execution, information on the latest government products and services, technical documentation, and community resources.

2.5.3.3 Tutorials and Demonstration Code

In addition to the detailed tutorials for developers published on the Singpass API portal, there are also demo applications and example code to illustrate the key implementation requirements. A dummy application, known as Mockpass, was built and made available as open source software on Github to allow developers to simulate Singpass and Myinfo transactions in a development environment.

Figure 2.5.3.3.1 Developer Tools: Signature Verifier



Signature Verifier

This utility tool is provided to help you verify the token or person signature against the Base String using the provided Public Certificate.

Formulated Base String

Base String generated by your application that will be signed using your private key.

```
POST&https://test.api.myinfo.gov.sg/com/v3/token&app_id=STG2-MYINFO-
SELF-TEST&client_id=STG2-MYINFO-SELF-
TEST&client_secret=44d953c796cccebcec9bdc826852857ab412fbe2&code
=e95d4003-303d-47b7-9427-
```

Digital Signature

Signature produced by signing the above Base String with your private key.

```
kXddcilil/13vc38emDveJGWqnjPOzSw2Ew9mYGSOF27BqwNUzb+pAOnT192Ju
novyVU1jo5RfxHwRBm4O4XdE12hBZfh4PvZCXT86WBPO680ZSTpFfLIHy8/F5q6S
aE++ADMqg5KVemz9HO4rzWkHt6VkHcRYHpqGz5RBlNsxqKGKsdjY9HEGas4h3
WkaCIVn/kMJ68IbVU3QFA/B84qSfSzvgtk3OwcRBJnPTWrKafRBMvvNCEtkuYOc
```

These tools and code examples are also of great value to raise awareness in the developer community and assist the rapid onboarding of new services. Developers also have access to "sandbox" APIs and developer tools (figure 2.5.3.3.1) that allow them to create functioning applications without the need for real Singpass users.

[13] For information regarding the Singapore Government Developer Portal, see: https://www.developer.tech.gov.sg/

3 GOVERNMENT DATA SHARING PLATFORM – API EXCHANGE (APEX)

3.1 Overview of APEX

The ability to seamlessly and securely data is key for digital service delivery. In 2016, the government introduced a policy to split government and public-facing digital services, leading to the requirement for a bridge or gateway allowing government agencies to share data from intranet to internet-facing services. This was the catalyst for the development of a data sharing platform.

Following this decision, APEX was launched in 2017 to become the bridge between intranet and internet zones in the government network architecture, enabling agencies to share data through application programming interfaces (APIs) from the intranet to internet zone services. APEX itself acts as an API gateway where agencies can consume approved APIs for secure and seamless access to data across government.

APEX enables centralized publication, cataloguing, discovery (as a self-service model), monitoring, and security management for the APIs. In doing so, it plays a key role in the Singpass ecosystem. Furthermore, Singpass (through the Myinfo product) provides citizens and residents with control over the sharing of their personal data, which occurs through APEX in the case of government services.

When APEX was initially developed, there was no government cloud policy, hence the system was developed in-house as an on-premise solution based on the Akana API management platform (a commercial API management platform). Now, APEX cloud is being developed for less-sensitive datasets. Moving to the cloud also opens the possibility of creating an API marketplace with the private sector.

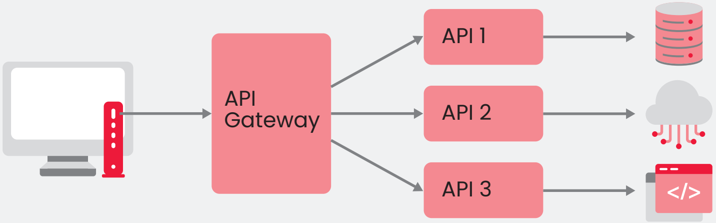
APEX is part of the Singapore Government Technology Stack (SGTS), a suite of shared and re-usable software components and infrastructure maintained by GovTech to enable government agencies to build digital services. Other examples of components of the SGTS include Singpass and the Government on Commercial Cloud (GCC). The SGTS is part of a broader framework known as Core Operations Development Environment and eXchange (CODEX), which is a shared digital platform between government agencies and the private sector for the development of better, faster, and more cost-effective digital services.

Box 3.1 What is an Application Programming Interface (API)

An API is a way for two or more software components to communicate with each other, including to transmit data. More specifically, an API is programming code that governs the access point to an application, which may be able to access a database. For example, if you search for a flight on a website, that website would use APIs to send a request to airlines and receive a response with offers. Well-designed APIs enable government agencies to enable access to their systems and databases for authorized users (e.g., other government agencies) while maintaining security and control.

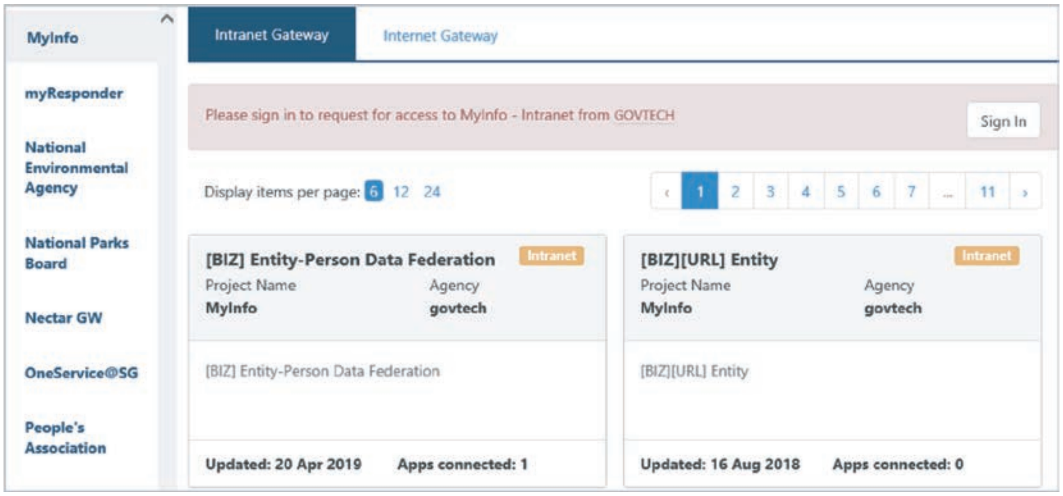
An API gateway sits between a user and a collection of APIs and back-end services. An API gateway can accept and aggregate API calls (essentially message asking an API to provide a service or data). It is also a management tool, enabling access control and monitoring of API usage. Using the example of searching for flights, a website may access the APIs of multiple airlines and travel agencies through an API gateway.

Figure B3.1
Illustration of How an API Gateway Works



Using APEX, developers of a requesting government agency can discover APIs, apply for access, and then pull data from various agencies on demand, with pre-configured access controls set by the data source agency. A central logging system provides an overview of all API logs, allowing monitoring and trouble-shooting when necessary.

Figure 3.1 Screenshot Example of the APEX API Library



Please sign in to request for access to MyInfo - Intranet from GOVTECH

Display items per page: 6 12 24

[BIZ] Entity-Person Data Federation Intranet
Project Name: MyInfo
Agency: govtech
[BIZ] Entity-Person Data Federation
Updated: 20 Apr 2019 Apps connected: 1

[BIZ][URL] Entity Intranet
Project Name: MyInfo
Agency: govtech
[BIZ][URL] Entity
Updated: 16 Aug 2018 Apps connected: 0

Box 3.2 Comparing APEX to the X-Road Government Service Bus Approach

Singapore's API Exchange (APEX) and the X-Road software first developed by the Government of Estonia (and implemented in Estonia as "X-Tee") share a similar high-level objective: to facilitate secure, seamless, and transparent data sharing between and among databases and services. In doing so, both approaches enable the federation or decentralization of data, removing the need for centralized data storage as an approach to unlocking the benefits of this data. There are, however, key differences in how they achieve these outcomes.

APEX is an API gateway where entities (currently only government agencies) can consume approved APIs for secure and seamless access to authoritative data managed by government, and API providers can manage that access. This allows service providers to gather data required for specific transactions, as well as to gain consent from the user through Myinfo. It has minimal infrastructure. On the other hand, X-Road is an entire ecosystem that has strict onboarding rules and requires much more infrastructure.

Table B3.1 Comparison of APEX and X-Road Approaches to Data Sharing

APEX	X-Road
APEX is an API gateway — Enabling entities to share data via APIs and for consuming services to access approved APIs.	**X-Road is an ecosystem** — A community of organizations using the same instance of the X-Road software for producing and consuming services.
There is a central stack but not a formal operator — APEX is part of the Singapore Government Technology Stack (SGTS), a suite of shared and re-usable software components and infrastructure maintained by GovTech to enable government agencies to build digital services.	**There is a central operator** — The owner of the ecosystem, the X-Road Operator, controls who are allowed to join the community, and the owner defines regulations and practices that the ecosystem must follow.
There is a relatively lightweight onboarding process — Potential API providers (government agencies) must register with the APEX Portal before being able to submit APIs or publication. Registration is based on control of a government agency email account, but also requires authentication to the portal with 2FA.	**There is a strict onboarding process** — Joining an X-Road ecosystem requires going through an onboarding process. During the process, the identity of each organization and technical access point is verified using certificates that are issued by a trusted Certification Authority (CA). The identities are maintained centrally, but all the data is exchanged directly between a service consumer and a service provider.

3.2 How APEX Works

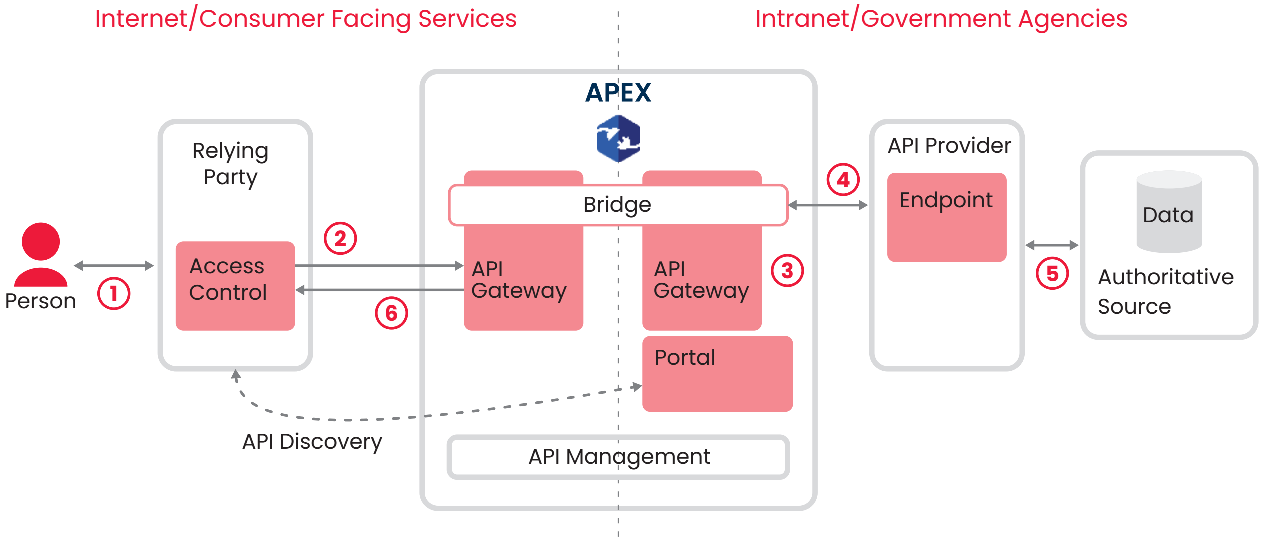
3.2.1 Components

APEX has two main components: the API gateway and the portal (used by API providers and API consumers).

- **Gateway:** serves the API traffic; provides orchestration, monitoring, throttling, and cybersecurity features
- **Portal:** allows providers to publish their APIs and for consumers of APIs to subscribe to their use

The portal is in the intranet zone and is used by API consumers and API providers. The purpose of the portal is to allow API providers to publish and configure their APIs on the portal, so that API consumers can discover APIs of interest to their services and subsequently subscribe to those APIs for use in their services. The gateway resides in both the intranet and internet zones (figure 3.2.1) and both services are due to move to the cloud in the next generation of APEX.

Figure 3.2.1 Overview of APEX Flow



At a high level, the steps in the APEX flow can be described as follows:

Step	Description	Notes
1	The user attempts to access a service.	Following authentication, user begins a transaction that requires trusted data.
2	The relying party (RP) requests additional data via API Exchange (APEX) based on user consent.	When a user accesses a service that needs trusted data to complete a transaction, the RP is able to request that data from an application programming interface (API) hosted by the gateway.
3	The API request is routed to the API provider via the bridge.	The bridge enables API calls to be placed with government API providers on the government intranet.
4	The API provider processes the request.	The API provider creates a response and sends this via the gateway for the originating RP.
5	Data is retrieved from the authoritative source.	Where required, data is retrieved from the authoritative source/database.
6	The response is routed back to the originating service.	The result of one or more API calls beyond the gateway is relayed to the originating service provider (RP).

3.2.2 Publishing APIs

Government agencies are responsible for the development of APIs to be published on APEX. API standards, however, are a relatively new addition to APEX and were first introduced in July 2021. Up until this point, agencies have been responsible for the design of the API interface based on their internal policies and best practices. This has not caused major problems, but as plans to extend the use of the API gateway have included the private sector, in addition to the move to a cloud-based version of APEX, there is an opportunity to introduce these API standards across the government as the platform evolves.

API standards have been published in conjunction with an instruction manual. These include:

- Versioning
- Documentation
- Recommended Use of the Open API Standard
- Lifecycle (for example, deprecation of APIs)

3.2.2.1 Provider Onboarding Process

Potential API providers (government agencies) must register with the APEX Portal before being able to submit APIs or publication. This is a relatively lightweight process, in which registration is based on control of a government agency email account, but it also requires authentication to the portal with two-factor authentication (2FA). Consumers use APEX to manage and request access to the APIs they need. In this case, the login mechanism is the same as providers; consumers are not charged for using APEX. Providers must also sign a service agreement outlining the charges levied by GovTech for the use of APEX.

Providers subscribe to APEX units (AU), which defines a soft limit on the number of transactions-per-second (TPS) that can be sustained (based on a 20KB payload). Subscribing to more APEX units increases the TPS. APEX provides non-production-grade APEX units at 50 percent cost for development and staging purposes.

The APEX cost model will be revised when it moves to the cloud, and this may result in a per API call model, rather than the existing fixed AU model, based on access to the on-premises services.

3.2.2.2 Supporting API Users and Providers

Consumers of APIs are largely supported by the publishing agency. The portal offers detailed documentation for developers, in conjunction with online training for API providers and consumers of APEX. A hotline is also provided by GovTech, although once onboarded, most providers become self-sufficient and use the provided tools to resolve issues.

3.2.3 Service Monitoring and Billing

Usage of APIs is measured in APEX Units (AU) which are calculated using the following guidelines: 20 transactions per second, 2–5 megabyte transaction size. Monitoring tools are provided to understand utilization and performance of APIs, so that peaks in traffic or potential issues can be identified automatically and managed accordingly. To protect the service at times of high load, APEX maintains a reserve capacity of 25 percent in order to maintain service levels.

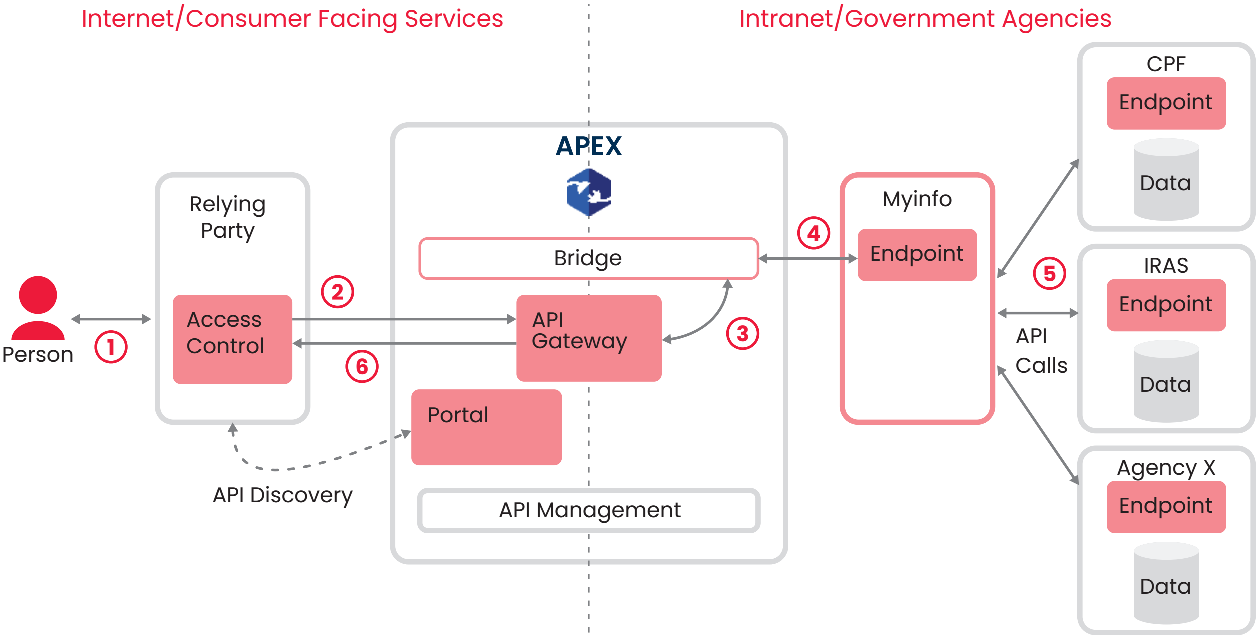
The use of APIs follows the use of services by the public. For example, services provided by the Immigration and Checkpoints Authority (ICA) to enable international travel will see peaks at key times, such as extended holiday periods. During these peak periods, where advance planning is possible, GovTech temporarily increases APEX resources to meet those peaks. However, the finite system resources in the current on-premises setup eventually limits scalability. This is one of the concerns that the next evolution of the platform intends to resolve, by tapping the cloud to increase agility in adapting to peak periods.

3.2.4 Myinfo and APEX

When users access a service that utilizes Myinfo for access to government data, the process of consent is handled automatically as Myinfo coordinates the gathering of government data via published APIs.

Myinfo acts as an aggregator and an orchestration point for service providers to request multiple data attributes relating to a single person. In this case Myinfo makes outward requests from the relevant API providers in government agencies, then collates the responses into a single response to be sent back to the initiating public-facing service (figure 3.2.4). All of this is made possible by the APEX portal and gateway, which facilitate the discovery and request of data, respectively.

Figure 3.2.4 APEX and Myinfo Flow



At a high level, the steps in the APEX and Myinfo flow can be described as follows:

Step	Description	Notes
1	The user attempts to access a service.	Following authentication, a user begins a transaction that requires trusted data.
2	The relying party (RP) requests additional data via API Exchange (APEX) based on user consent.	When a user accesses a service that needs trusted data to complete a transaction, the RP is able to request that data from an API hosted by the gateway.
3	Application programming interface (API) requests are routed to Myinfo.	A request for multiple data attributes is routed through the gateway to Myinfo (as an API call). *Note: During this step, the user will be prompted to consent to data sharing via the Singpass app.*
4	Myinfo routes API requests to relevant APIs.	Myinfo interprets the request for data and presents multiple corresponding APIs to the relevant authoritative sources (API providers).
5	Data is aggregated by Myinfo.	Myinfo aggregates responses received from the API providers and prepares a single response payload.
6	The response and data payload are returned to the RP.	The result of one or more API calls beyond the gateway is relayed to the originating service provider (RP).

3.3 Key Enablers

3.3.1 Authoritative Data and the Government Data Architecture

A key success factor for APEX (as well as for Myinfo) has been the identification of authoritative data (or “single sources of truth”) in government databases. Beginning around 2015, Infocomm Development Authority of Singapore (IDA) and, subsequently, GovTech, went through individual fields in key government datasets to identify the most reliable sources. For example, within the government, different datasets contained address-related data, but which one was the most trustworthy and up-to-date source? The residential address was found to be from ICA, income details from the Inland Revenue Authority of Singapore (IRAS), and marriage status from the Registry of Marriages. Once identified and established as re-usable, the government does not need to ask for the same information multiple times.

Similarly, the development of the Government Data Architecture has led to a whole-of-government (WOG) approach to data standards and formats, facilitating interoperability and comparability of information at a technical level.

This practice of “Tell us once” will not be the same in every country, but the principle of identifying and assessing the authoritative source for each key data attribute is a vital component for its successful implementation in government data sharing. From the citizen perspective, this practice of “Tell us once” has a tremendously positive effect, reinforcing the perception that government is a single entity, and that if an individual informs one part of government that their data has changed, that message should reach all parts of government.

In addition to analyzing the data and how it was validated, a parallel discussion examined whether this data should be held in a central data store. The conclusion was that this approach creates a risk, as it is very attractive for attackers; but also, if such a data set were created, there is the problem of which agency would own and protect it. There is also the problem of a central dataset being simply a snapshot of the data held elsewhere—a point in time value—so this would run the risk of becoming out-of-date if it were not constantly updated. The resulting policy was that the key data attributes, or the single sources of truth, should remain under the control of the agency that has a vested interest in that data. This implies that the means of accessing that data are created to enable the wider utility.

This thinking led to the first implementation of Myinfo for an individual to give consent to sharing their verified data in government-to-person transactions, as well as Myinfo business for an authorized officer to consent to sharing their verified data in government-to-business transactions. Beyond government, this has also enabled many transactions that were previously process-heavy and paper-based experiences to be entirely digital, such as opening a bank account. In this model, financial institutions can request multiple relevant data attributes, which the customer has the right to consent to (or decline), and APIs facilitate data transfer from the government to the financial institution, as triggered by user consent. Furthermore, Myinfo has led to the creation of many other digital products made possible by the underlying trust that individuals have in Singpass.

Alongside APEX as a single point of exchange for data from government agencies, strong governance, data standards, discoverability, and common catalogues were developed. This means that today, APIs and an API gateway exist, giving access to various different data items from across government agencies, enabling rich user journeys and digital transactions.

3.3.2 Ensuring Integrity and Trust

As API messages pass between the intranet and internet zones, controls are in place to detect attacks through deep packet inspection and checks on the high-level metadata of request and response headers.

The messages themselves are protected according to the API specification of the API provider. Some providers may enforce encryption or the signing of data payloads to ensure integrity—APEX provides mechanisms for this but is not a requirement to use the gateway. This also extends to the security of APIs, such as the requirement for API keys, and any limits on use that the provider may enforce.

Since its launch in 2017, APEX was quickly viewed as significant national infrastructure, or SII. This status has strongly increased the compliance overhead costs for the service, but this has been embraced by the GovTech team and their operations.

3.3.3 Securing API Transactions

APEX and its API transactions are monitored through the Cyber Watch Centre (CWC), for central security monitoring which utilizes security information and event management (SIEM) tools and techniques to provide real-time analysis of network traffic and alerts when security incidents are detected. The APEX system also incorporates other tools to audit events and logs for issues and abnormal activity.

The data payloads carried in API transactions are secured according to the specifications put in place by the API provider. This means that there are currently no set standards for data integrity or confidentiality of API calls; instead, it is the responsibility of the agency publishing an API that gives access to data to ensure that appropriate controls are in place.

The responsibility of API providers is made clear in a service agreement that is put in place when an API is added to the APEX API gateway. GovTech advises on good practices and clearly states the responsibilities of each entity (agency) as it interacts with the wider Singpass and APEX ecosystems.

3.3.4 Data Protection and Privacy

APEX is focused on data exchange for digital transactions and does not reach back further into agency-to-agency transactions where the user is not present (online or offline), which is the case for government service buses (such as X-Road). As a result, APEX is more practical and less complex to implement, as it focuses on surfacing standardized APIs for data sharing, thereby solving a specific problem, rather than creating a comprehensive infrastructure for digital government.

4 IMPACT

4.1 Singpass Adoption

Despite being an optional product, Singpass currently has a very high adoption rate among citizens, residents, and relying parties. As of August 2022:

- There are more than 4.5 million users, covering 97 percent of citizens and residents aged 15 and above.
- Over 2,000 services offered by more than 700 government agencies and businesses, utilize Singpass to support relevant use cases, ranging from financial services to healthcare, education, business services, and transport. 900 of these services have been onboarded to Myinfo.
- More than 350 million personal and corporate transactions are facilitated using Singpass every year. Myinfo sees about 200,000 transactions a day on average.
- The document wallet and digital identity card (IC) are accessed approximately 485,000 times per month.

4.2 API Exchange (APEX) Adoption

The number of application programming interfaces (APIs) supported through APEX has risen above 4,000 and originates from over 45 different government agency projects. 35 government agencies consume these APIs. The level of traffic experienced has crossed 100 million transactions per month, with peaks exceeding 300 million transactions per month.

4.3 Convenience and Cost Savings

Singpass and APEX have contributed to significant increases in convenience for citizens and residents, as well as productivity gains and cost savings for government agencies and businesses. For example, most government services in Singapore can be accessed completely online; this includes registering a birth via the LifeSG application. It has also boosted the resilience of Singapore, as evidenced by the ability of the government to quickly develop new products for the public health and economic response to the COVID-19 pandemic.

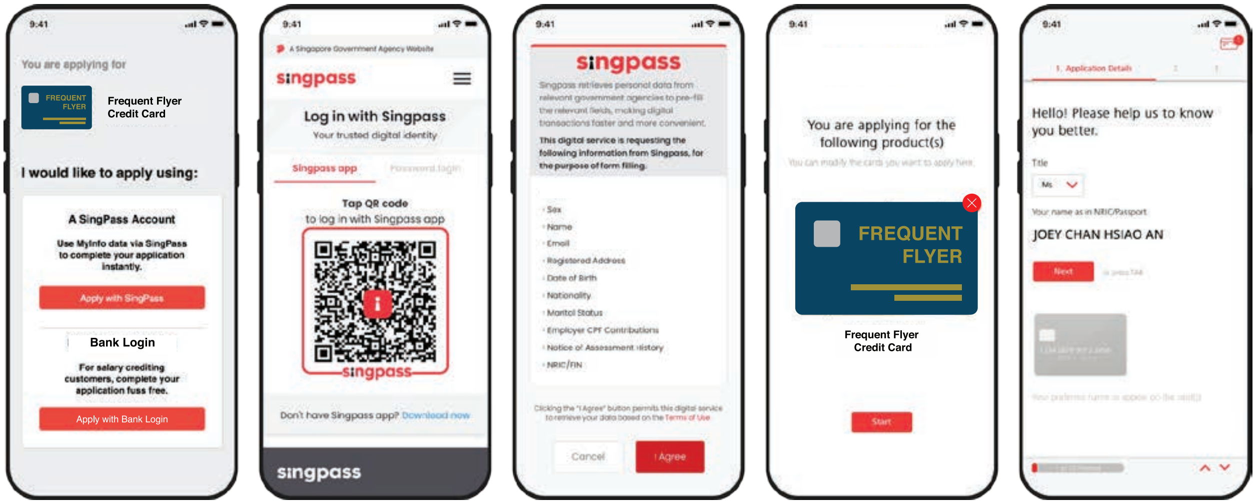
There has been a significant reduction in process steps required for some transactions. For example, Myinfo (enabled by APEX) has reduced the number of "clicks" to open a bank account—in other words, the number of steps in the process—by almost 100 in some cases. This has a direct impact on customers and financial service providers, as customers are more likely to complete the process, and the overhead cost for the provider is greatly reduced. According to GovTech, Myinfo has resulted in an average decrease of up to 80 percent in application time for users, with businesses reporting up to a 15 percent higher approval rate, due to better data quality and significant cost savings in their customer acquisition process.

4.4 Example Use Cases

4.4.1 Easy Customer Onboarding — Instant e-Know Your Customer (eKYC)

Financial services are a high-value use case for national digital identity (NDI) in any country. GovTech has worked closely with the central bank, the Monetary Authority of Singapore (MAS), to create an enabling environment for financial institutions to adopt Singpass. Myinfo enables financial service providers to carry out instant and consent-based onboarding of new customers, satisfying customer due-diligence requirements of MAS. The introduction of Identiface has provided additional authentication assurance, further reducing risks for financial service providers.

Figure 4.4.1 Example of How Myinfo Can Be Used to Apply for a Credit Card Instantly



You are applying for

Frequent Flyer Credit Card

I would like to apply using:

A SingPass Account

Use MyInfo data via SingPass to complete your application instantly.

Bank Login

For salary crediting customers, complete your application fuss free.

A Singapore Government Agency Website

Log in with Singpass

Your trusted digital identity

Tap QR code to log in with Singpass app

Don't have Singpass app? Download now

Singpass retrieves personal data from relevant government agencies to pre-fill the relevant fields, making digital transactions faster and more convenient.

This digital service is requesting the following information from Singpass, for the purpose of form filling.

- Sex
- Name
- Email
- Registered Address
- Date of Birth
- Nationality
- Marital Status
- Employer CPF Contributions
- Notice of Assessment History
- NRIC/FIN

Clicking the "I Agree" button permits this digital service to retrieve your data based on the Terms of Use

You are applying for the following product(s)

You can modify the cards you want to apply here.

Frequent Flyer Credit Card

Hello! Please help us to know you better.

Title

Ms

Your name as in NRIC/Passport

JOEY CHAN HSIAO AN

Policy guidance changes to the financial sector were made by MAS in 2018 to support the use of Singpass as a non-face-to-face verification measure, including making it clear that financial institutions would not be expected to separately obtain physical documents or a photograph if they used Myinfo for their KYC process.[14] However, this was not necessarily needed; in the first instance, financial institutions saw the opportunity to make improvements to their productivity and customer acquisition soaring as a result of access to automated identity verification and trusted data obtained directly from government sources.

4.4.2 Digital Government Services — LifeSG and Birth Registration

Singpass and APEX work together to respectively support the front- and back-end processes of LifeSG, Singapore's integrated digital government services application. Singpass enables account creation, while APEX facilitates the exchange of information that allows the user experience, including notifications and services offered on LifeSG, to be personalized.

A good example of this is how birth registration is managed end-to-end online through the LifeSG application and is subsequently integrated with support for new-borns provided by the government, including a baby bonus, the opening of a Child Development Account (CDA), and a free library membership. In 2022, the Immigration and Checkpoints Authority (ICA) launched digital birth (and death) certificates, which can be downloaded at the end of the process. The digital certificates contain a digitally signed QR code that can be easily verified through ICA.

4.4.3 COVID-19 Response — SafeEntry and TraceTogether

When the COVID-19 pandemic triggered the need for contract tracing in early 2020, countries across the world scrambled to develop digital systems that would support checking into and out of venues and public spaces efficiently, inclusively, and in a privacy-preserving manner. In Singapore, GovTech was able to leverage several elements of the Singapore Technology Stack (SGTS), including Singpass, to develop the SafeEntry system. Initially, SafeEntry was an application that allowed venues to scan the barcode or QR code on the back of National Registration Identity Cards (NRICs) and other ICs.

SafeEntry gradually evolved to become an ecosystem based on citizens and residents scanning unique QR codes to check into and out of venues, first as a feature in Singpass and then through the new TraceTogether contact-tracing application. GovTech also leveraged Corppass to enable businesses to easily

[14] Monetary Authority of Singapore. 2022. AMLD 01/2018: "Use of Myinfo and CDD Measures for Non Face-to-Face Business Relations." https://www.mas.gov.sg/regulation/circulars/circular-on-use-of-myinfo-and-cdd-measures-for-non-face-to-face-business-relations

log in to the SafeEntry portal to generate their QR code. For citizens and residents without a smartphone or the corresponding TraceTogether app, a TraceTogether token was also made available, which could be worn and scanned by an agent at the venue in a manner similar to the app.

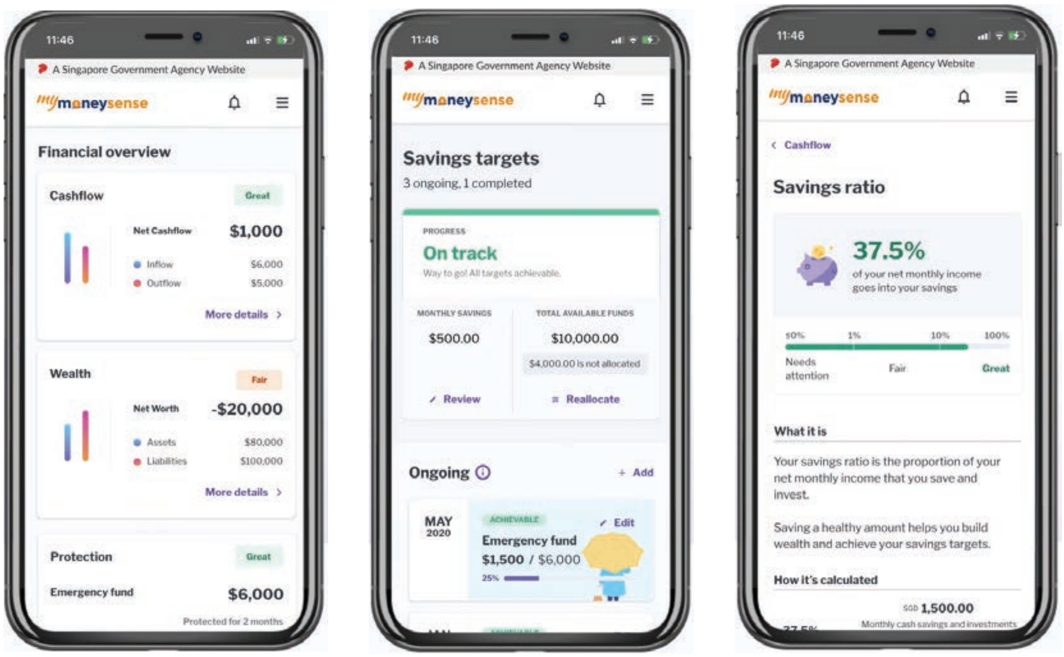
4.4.4 Enabling Data Infrastructure — Singapore Financial Data Exchange (SGFinDex) and Singapore Trade Data Exchange (SGTraDex)

Developed by the Monetary Authority of Singapore (MAS) and the Smart Nation and Digital Government Group (SNDGG) in collaboration with The Association of Banks in Singapore and seven participating banks, SGFinDex tackles the problems associated with financial information for individuals spread across multiple institutes and government agencies.

Using Singpass to correctly identify individuals, SGFinDex provides a centrally-managed online consent system that can be utilized by multiple providers. The user can then access their financial information held across different government agencies, as well as financial institutions, through secure apps, thereby consolidating and simplifying their finances.

Users access SGFinDex by first connecting to their bank online or through the MyMoneySense service (a financial planning digital service jointly developed by the Ministry of Manpower (MOM) and GovTech (figure 4.4.4). Once logged in,

Figure 4.4.4 Accessing Financial Data with MyMoneySense and SGFinDex



11:46
A Singapore Government Agency Website
mymoneysense
11:46
A Singapore Government Agency Website
mymoneysense
11:46
A Singapore Government Agency Website
mymoneysense

Financial overview

Cashflow — Great

Net Cashflow $1,000

Inflow $6,000

Outflow $5,000

Wealth — Fair

Net Worth -$20,000

Assets $80,000

Liabilities $100,000

Protection — Great

Emergency fund $6,000

Protected for 2 months

Savings targets

3 ongoing, 1 completed

PROGRESS

On track

Way to go! All targets achievable.

MONTHLY SAVINGS $500.00

TOTAL AVAILABLE FUNDS $10,000.00

$4,000.00 is not allocated

MAY 2020 — ACHIEVABLE

Emergency fund

$1,500 / $6,000

25%

Savings ratio

37.5%

of your net monthly income goes into your savings

What it is

Your savings ratio is the proportion of your net monthly income that you save and invest.

Saving a healthy amount helps you build wealth and achieve your savings targets.

How it's calculated

SGD 1,500.00

Monthly cash savings and investments

users can opt to approve the connection of the bank to SGFinDex, enabling the secure retrieval of financial information from the bank and Myinfo.

Since its inception on December 7, 2020, SGFinDex has spurred financial planning among participating bank customers with over 150,000 unique user sign-ups, 290,000 bank accounts linked, and 620,000 data retrievals made.

Similarly, the Singapore Trade Data Exchange (SGTraDex) is a public-private initiative that seeks to address inefficiencies in supply chain documentation and information flows for international trade.

This initiative has highlighted a number of key use cases in which digital technology can provide efficiencies. These include:

- Strengthening Trade Finance and Converging Efficiencies
- Container Flow Node Decongestion
- Bunker Optimization
- Green and Sustainable Trade Finance
- Ship Supplies and Lighterage Optimization
- Demurrage Management and Optimization

To solve these key supply chain issues and create a stronger and more robust supply chain ecosystem for international trade flows, SGTraDex provides a common data infrastructure and easy-to-use digital tools for shippers, traders, logistics Operators, financial institutions, and associated organizations, such as regulators and associations.

5 THE FUTURE OF SINGPASS AND API EXCHANGE (APEX)

5.1 Decentralization and Alternative Trust Anchors

GovTech is actively exploring the potential of federated and decentralized identity models for Singpass. How they could be accommodated by Singpass in the future will undoubtably influence future iterations of Singapore's national digital identity (NDI) ecosystem. Alternative trust anchors may also be considered, particularly for a decentralized model where user data may not be obtained directly from an application programming interface (API), but more likely shared by the user directly with a service.

5.2 Authorization

Currently, Singpass is used for onboarding. GovTech will soon offer businesses the opportunity of using Singpass as a means for their customers to remotely authorize transactions based on the strong user authentication and verification provided by the NDI. An example might be a push notification from a banking application to authorize a payment.

5.3 Expanding the Digital Wallet

Currently, there are plans to expand the number of digital documents that can be held in the Singpass wallet. Each of these would be implemented in a similar manner to the digital ID card (IC), driving license, and COVID-19 tests and vaccination certificates, including the ability to selectively disclose information and to provide adequate security controls to prevent duplication.

Likely candidates for inclusion are as follows:

- **Identity-related cards,** such as government-issued driving credentials and military identification cards
- **Vocation-related cards,** such as commercial driving credentials and medical practitioner certifications
- **Benefits-related cards,** such as those issued for healthcare subsidies or for the elderly

5.4 Delegation

Individuals do not just interact with the government and businesses for themselves. They may also need to act on behalf of others, such as elderly parents and family members with less digital literacy. Through user research, GovTech found that families would address this by pragmatically passing around the password and hardware token of the individual who they were transacting for. GovTech is exploring ways of integrating 'digital delegation' into Singpass, so that there can be easier ways for users to more securely delegate trusted family members to transact digitally on their behalf.

5.5 Cross-Border Interoperability

Singapore has been working with a number of countries to explore cross-border use cases for digital identity. Digital identity is a part of the digital economy agreements signed with Australia and the United Kingdom, and in June 2022, the Singaporean Ministry of Trade and Industry (MTI) collaborated with the Association of Southeast Asian Nations (ASEAN) Secretariat to convene Southeast Asia's first regional digital identity workshop.

5.6 Expanding APEX for the Private Sector

APEX users are currently government agencies; however, there is increasing demand to support government-to-citizens (G2C) and government-to-business (G2B) use cases. APEX has started exploring such use cases with the advent of the APEX Cloud Pilot, which will also include access to APIs for private sector service providers. During the pilot phase, these businesses will be invited by government agencies to participate. It is expected that the eventual rollout and widening of access to government data is likely to be met with great interest in a country where digital services are already accepted as the norm.

5.7 APEX Moving to the Cloud

The APEX API gateway will move from a virtual machine (VM) based architecture to a containerized design in the cloud in the next version of APEX. The current on-premises, hosted VM-based architecture has grown to over 700 VMs, which requires significant cost and effort to maintain. The cloud-based version aims to reduce this issue.

The cloud version of APEX is planned to go live in March 2023, starting with a pilot for external businesses and three major agencies in July 2022. The pilot will feature APIs fronted by the APEX Cloud gateway and published on the API marketplace, for whole-of-government (WOG) and select private sector service providers. Meanwhile, the on-premises system will remain active to support confidential APIs that cannot be shared beyond central government services.

6 SUCCESS FACTORS AND LESSONS

National digital identity (NDI) and government data sharing platforms, just like any digital government solutions, rarely map directly from one country to the needs of another country. Each country has its own particular ways of working, including institutional arrangements, legal frameworks, attitudes towards data protection and privacy, and requirements for ID form factors (such as smartcards, mobile, digital credentials, etc.). In other words, there is no one-size-fits-all approach.

Singapore is a small and prosperous country with a strong, well-funded technology capability at the heart of government: GovTech. Many countries are not in this position, which may make it more difficult to implement similar solutions to Singpass and API Exchange (APEX). However, it should be recognized that GovTech, similar to the Singpass and APEX products, has taken several years to mature and has solved many of the problems that other countries will encounter, such as technology choices, user adoption, and working with the private sector. GovTech has been keen to share its experiences and takeaways related to building digital government, which will benefit many other countries.

Any country wishing to build their own NDI and government data sharing platform should consider their own domestic requirements and circumstances and then adapt or learn from the experience of Singapore and other countries. They should not directly replicate any other approach. Equally, key building blocks for success should always be observed, such as ensuring that critical legislation is in place for enabling new systems and for data protection; that government agencies have the relevant skills and coordination to manage implementation effectively and efficiently; clearly identifying the risks and putting in place mitigation measures; and understanding the needs of vulnerable populations, including those on the fringes, and acting on that understanding.

This section summarizes some of the key success factors and lessons from the Singpass and APEX experience to date.

6.1 Evolution

An underlying characteristic of the approach taken in Singapore with regard to Singpass and APEX is one of achievability. There has not been a rush to implement multiple capabilities in one huge implementation, but instead a measured approach has been taken, starting with Singpass as a sign-in to government services, followed by development of application programming interface (API) gateways, enabling access to authoritative sources of data (for example, Myinfo), and then the steady addition of new products for citizens and residents, such as document signing, face verification, and the soon-to-come remote authorization of transactions.

Lessons have also been learned along the way, thereby improving the usability and security of Singpass. For instance, the username could initially be set by users until, problems arose with regard to users remembering their username. As a result, the username was shifted to the National Registration Identity Card (NRIC) number or Foreign Identification Number (FIN).

This approach of solving a key problem, then constantly building on that platform has improved confidence in users and relying parties (RPs).

6.2 Prioritizing User Experience and Understanding the Needs of All Segments of Society

GovTech invests heavily in user experience across the development life cycle, ingraining it not as a luxury, but as a prerequisite. All products and services are tested with key stakeholder groups, including populations vulnerable to digital exclusion, such as persons with disabilities and the elderly. Integrated into the "Agile" process, it also ensures that products meet the needs of users through user feedback. The result is very high usability and user-friendliness, as is evident by the overwhelmingly positive feedback for the Singpass application on the Google Play Store (a 4.7 average rating from 96k reviews) and iOS App Store (a 4.8 average rating from 3.8k reviews).[15]

6.3 Focusing on Use Cases and Value

The GovTech adoption strategy for Singpass has been to focus on specific sectors that require high level of trust. The majority of the time, these sectors are regulated and observe the greatest impetus to integrate with Singpass and digitally transform their agencies and businesses. With the adoption and success of Singpass, the focus will gradually expand to other sectors rather than trying to solve every sector problem from the program's initiation. Similarly, adoption of APEX has been driven by demand for information from other government agencies.

[15] Ratings as published by the Google Play Store and iOS App Store on August 2022.

6.4 Identifying Authoritative Data

One of the key enablers for both Singpass and APEX was the exercise of developing the Government Data Architecture and identifying authoritative databases as “single sources of truth” for each specific attribute. The Government Data Architecture, in particular, created common whole-of government (WOG) standards and formats. This facilitates interoperability and data accuracy, as well as greater privacy (as data is not replicated in multiple databases). However, Singapore was able to accomplish this without causing any undue exclusion because it has universal coverage of its foundational ID system, as well as accessible mechanisms for citizens and residents to address any problems with their data. It may be challenging for most other countries, particularly those with larger populations and more complex conditions, to have a “single source of truth” and thus, these countries may need to have more flexibility.

6.5 Foundational ID

Both Singpass and APEX benefit significantly from Singapore having a strong foundational ID system. Singpass was a natural extension of the existing foundational ID system. All citizens have an NRIC number from birth, and residents have a FIN from arrival. It is also made easy by ICA and MOM to verify this information. For many countries that do not have a foundational ID system, the basis for a digital ID is much harder, as the identity proofing and onboarding processes are more complex. This is the case in the UK and Australia, for example, where multiple touchpoints are required to prove identity when creating a digital ID. This can lead to friction and exclusion.

With respect to APEX, the NRIC number and FIN each provide a unique key that facilitates the unique identification and matching of information across databases.

6.6 Technology and Required Skillsets

GovTech and its predecessor, Infocomm Development Authority of Singapore (IDA), have adopted technologies that promote interoperability and are, where possible, open in nature—such as Open ID Connect for the authentication protocol of Singpass. Relying party services are therefore able to utilize any technology or product they see fit in order to build their systems, as long as they are able to make requests using Open ID Connect and process corresponding responses in Singpass documentation.

APEX, including its gateway, was originally developed based on a commercial API management platform, and while initially implemented on-premises, is currently being redesigned for the cloud. This implies a strong internal capacity and skills for secure hosting, as well as information security and cyber security expertise to ensure the safety and assurance of cloud-based services.

6.7 Adopting Technologies Responsibly

Singapore has adopted new technologies and techniques as they become relevant, rather than as they become available. An example of this is the current approach of the Singpass application: It is not decentralised and does not rely on distributed ledgers. It is a secure means of access to services that some may argue takes control away from the user. However, in this case, that does not appear to have happened, and the power of tools such as Myinfo, as well as their rapid adoption, have attested to this.

It should also be noted that, although the Singpass team initially chose the centralized model with Myinfo, they are also constantly reacting to changing user requirements and sentiments. For example, in response to the increasing need for user privacy (that is, users not wanting the government to know which RPs they share data with), the Singpass team is starting to explore a decentralized model of data sharing and how that may function in the future.

THE WORLD BANK
IBRD • IDA | WORLD BANK GROUP

ID4D
IDENTIFICATION FOR DEVELOPMENT

GOVTECH
SINGAPORE