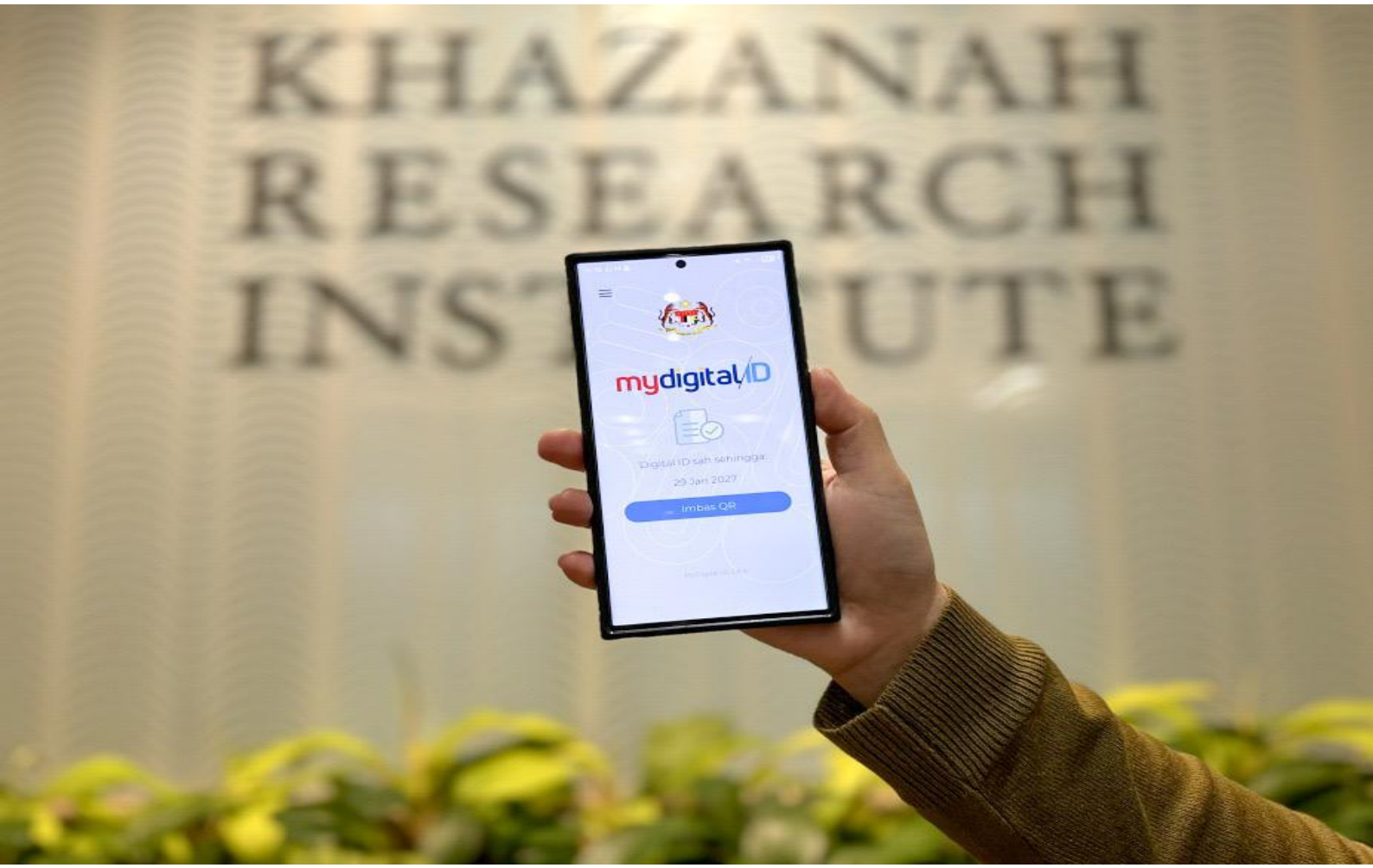
KHAZANAH RESEARCH INSTITUTE

DISCUSSION PAPER 07/25 | 28 JANUARY 2026

Assessing and Optimising MyDigital ID

SALBIAH IDRIS



Khazanah Research Institute

The **KRI Discussion Papers** are a series of research documents by the author(s) discussing and examining pressing and emerging issues. They are stand-alone products published to stimulate discussion and contribute to public discourse. In that respect, readers are encouraged to submit their comments directly to the author.

The views and opinions expressed are those of the author and may not necessarily represent the official views of KRI. All errors remain author's own.

DISCUSSION PAPER 07/25 | 28 JANUARY 2026

Assessing and Optimising MyDigital ID

This discussion paper was prepared by Salbiah Idris (Research Associate) from the Khazanah Research Institute (KRI). The author is grateful for valuable comments from Mr Sam Ng, Knowledge Management and Community Officer, Sinar Project; Dr Mohd Ruzeiny Kamaruzzaman, Director of Stakeholder Management and Government Affairs, MyDigital ID Sdn. Bhd.; Dr Rachel Gong, Deputy Director of Research, KRI; and Dr Jun-E Tan, Senior Research Associate, KRI.

The author would also like to thank Dr Mohd Ruzeiny Kamaruzzaman, Director of Stakeholder Management and Government Affairs, MyDigital ID Sdn. Bhd.; and Mr Ng Kang Siong for their time and for being interviewed on the MyDigital ID initiative. Appreciation is further extended to Nur Sofea Hasmira Azahar for assistance with formatting and presentation of the paper.

The views and opinions expressed in this paper are those of the author and may not reflect the official position of KRI.

Author's email address: **salbiah.idris@krinstitute.org**

Published 28 JANUARY 2026. Published by Khazanah Research Institute at Level 17-1, Mercu UEM, Jalan Stesen Sentral 5, Kuala Lumpur Sentral 50470 Kuala Lumpur, Malaysia. Tel: +603 2705 6100; Fax: +603 2034 0000; Email: enquiries@KRInstitute.org.

Cover photo by Belinda Liew Ai Ching.

DISCUSSION PAPER 07/25 | 28 JANUARY 2026

Assessing and Optimising MyDigital ID

SALBIAH IDRIS

Summary

Malaysia's MyDigital ID represents an important step in the country's efforts to develop a trusted, inclusive and secure digital identity ecosystem. Launched in November 2023, MyDigital ID currently serves as a Single Sign-On (SSO) authentication platform, allowing users to access government and private sector digital services using a single credential. It complements MyKad and forms part of the broader MyDIGITAL Blueprint, which seeks to modernise public service delivery, reduce administrative duplication and strengthen national digital infrastructure.

International experience indicates that while authentication platforms can improve access and efficiency, the broader effectiveness of national digital identity systems depends on legal clarity, institutional governance, inclusion and public trust, in addition to technical design. Systems that remain focused primarily on authentication may encounter limitations in adoption, interoperability or legitimacy if these enabling conditions are not progressively addressed. As Malaysia expands the use of MyDigital ID, policy choices over time are likely to influence how the platform develops and how it is perceived by users and service providers.

This discussion paper has three objectives. First, it identifies key determinants shaping the effectiveness of national digital identity systems, drawing on frameworks developed by internationally recognised organisations. Second, it evaluates Malaysia's MyDigital ID against these determinants through a qualitative and comparative policy analysis. Third, it outlines policy considerations that may support the continued development of MyDigital ID in a manner that is inclusive, trusted and sustainable.

Based on international frameworks and comparative case studies from Estonia, Singapore and India, the analysis identifies five determinants of effectiveness:

i. integrity of registration and credentialing;
ii. functionality and interoperability;
iii. governance, oversight and safeguards;
iv. inclusivity and accessibility; and
v. sustainability and system design.

Across different national contexts, digital identity systems that perform well tend to share several characteristics, including a clear legal basis defining roles and responsibilities, coordinated institutional arrangements, privacy and security safeguards embedded by design, inclusive access models that address digital divides, and interoperable technical architectures that enable safe reuse of identity credentials across services. International experience also highlights that

public trust is shaped by governance and accountability mechanisms as much as by technical assurance.

The assessment finds that MyDigital ID demonstrates several strengths at its current SSO stage. Its design incorporates recognised security standards, applies privacy-by-design principles and relies on authoritative verification against government databases. Governance responsibilities are distributed across multiple institutions, and adoption has increased as more digital services are integrated. At the same time, the analysis highlights areas where further clarification or development could strengthen longer-term effectiveness, including the legal basis for digital identity, transparency around oversight and redress mechanisms, inclusion outcomes, and long-term interoperability and sustainability arrangements.

In this context, the paper identifies five policy areas for consideration: strengthening the statutory framework for digital identity, enhancing institutional coordination and accountability, supporting public trust through transparency and engagement, developing a more explicit inclusion and accessibility strategy, and reinforcing technical resilience through open standards, interoperability governance and sustainable funding. These considerations provide a structured framework for evaluating how MyDigital ID can continue to evolve within Malaysia's broader digital governance landscape.

Table of Contents

1. Introduction

1.1. Defining Digital Identity

Digital identity commonly refers to a secure, electronically verifiable set of personal attributes and credentials that allow individuals to prove who they are across both digital and physical environments[1]. It is distinct from ordinary online accounts because it is anchored in verified data issued or recognised by an authoritative body, often carrying legal effects for authentication and electronic signatures[2]. When properly implemented, a digital identity system provides a reliable means for individuals to access essential services, assert rights and participate securely in economic and civic life[3].

In practice, digital identity supports functions as diverse as healthcare registration, social-welfare disbursement, education enrolment, tax filing and banking verification. It enables citizens to authenticate remotely, complete transactions in seconds, and authorise the sharing of verified information without the need to repeatedly submit physical documents. The system thus becomes an enabling layer of national digital governance by reducing administrative duplication, improving record accuracy, and expanding inclusion for those previously marginalised by distance or bureaucracy[4].

Digital identity is increasingly recognised as part of digital public infrastructure (DPI) alongside digital payments and secure data-exchange frameworks, forming the foundation of a trusted digital state[5]. Yet, as international practice shows, the same technology that empowers can also centralise control, raising concerns about surveillance, privacy and exclusion[6]. Effective systems, therefore, depend on embedding not only cryptographic strength but also institutional and legal safeguards that ensure transparency, consent and accountability[7].

1.2. Global Momentum in Digital Identity

Worldwide, governments are implementing digital identity systems as key tools for driving digital transformation and fostering economic growth. As of October 2025, a total of 168 countries had established digital ID systems, of which 117 had operational authentication mechanisms and within this group, 72 countries had fully implemented systems with at least two sectoral use cases[8]. This global spread reflects two main motivations. First, digital identity improves efficiency: it cuts transaction costs, supports accurate targeting of public subsidies and enables interoperable e-government services[9]. Second, it promotes inclusion: reliable identification allows people to access welfare, education and financial services[10].

---

[1] World Bank (2018c); WEF (2018); World Bank (2016)
[2] World Bank (2016); Dahan and Sudan (2015)
[3] Dahan and Sudan (2015); OECD (2011)
[4] World Bank (2016); WEF (2016); Dahan and Sudan (2015)
[5] World Bank (2025b); OECD (2024a); UNDP (2023a)
[6] World Bank (2025b); (2019); WEF (2018)
[7] Ibid.
[8] UCL IIPP (2025)
[9] World Bank (2016); Dahan and Sudan (2015); OECD (2011)
[10] Ibid.

However, global experience also reveals the dual nature of digital identity. When poorly managed, systems risk excessive collection of personal data, opaque surveillance or exclusion of those without proper documentation or connectivity[11]. International frameworks emphasise that rights-based design, interoperability and independent oversight are essential to balance innovation with protection[12]. These frameworks influence how emerging systems, including Malaysia's are evaluated.

1.3. Malaysia's Digital Identity Agenda

MyDigital ID, launched in November 2023, functions as an SSO authentication platform that allows users to access multiple public-sector portals with one credential[13].

The idea of a national digital identity was first raised in 2018 to complement the MyKad[14]. At that time, fragmented identity verification systems caused duplication of costs, lack of standardisation, risks to data security and a poor user experience with multiple logins. The proposed national digital identity aims to enable secure, efficient and trusted digital services, offering greater convenience for users, improving service quality and potential cost savings for government, and supporting service providers through streamlined processes and expanded opportunities[15].

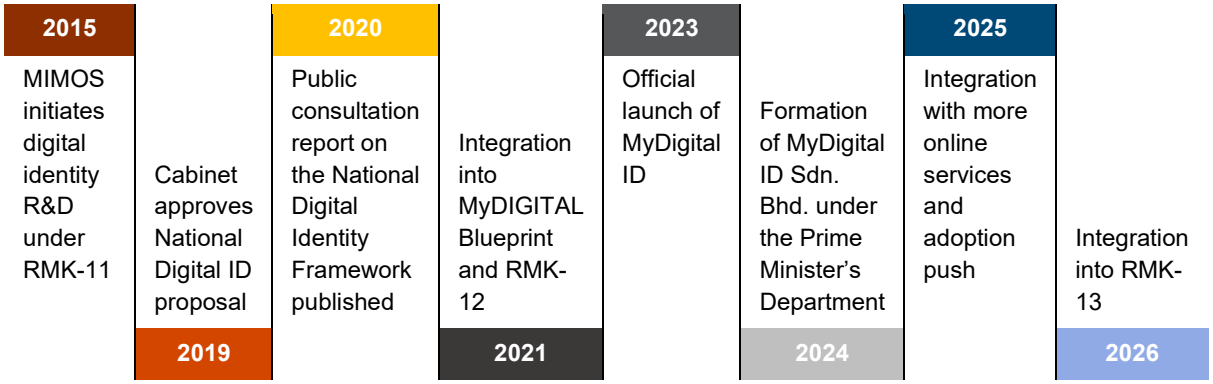
Policy direction originated in the Ministry of Communications and Multimedia (KKMM), which, through the Malaysian Communications and Multimedia Commission (MCMC), submitted the proposal for a National Digital Identity to the Cabinet on 8 May 2019[16]. Cabinet approval mandated MCMC to commission a feasibility study examining the policy landscape, implementation model, costs and benefits. The process included stakeholder consultation, ensuring the initiative addressed practical needs and sectoral concerns[17]. Public consultations discussed that ministries and agencies would form the first phase of integration, with regulated private sectors such as finance, telecommunications, healthcare and e-commerce to follow[18]. This phased rollout reflects a deliberate choice to build trust and capacity through government services before expanding to a wider audience. The study, completed in 2020, supplied the framework that was later integrated into the Malaysia Digital Economy Blueprint (MyDIGITAL) in 2021. MyDigital ID was introduced as a "platform of trust", designed to complement MyKad to provide a digital credential to support both government and private-sector transactions, and as proof of citizenship[19].

Under the Twelfth Malaysia Plan (RMK-12), the concept of Malaysia's national digital identity was introduced as a secure, integrated platform for identity verification and data sharing to enhance digital services, privacy and cybersecurity. Through a single trusted digital identity, it aims to

[11] Clark and Daly (2019); World Bank (2019)
[12] Clark and Daly (2019); WEF (2018); (2016); Dahan and Sudan (2015)
[13] My Digital ID Sdn Bhd (2025); Economy Planning Unit of Malaysia (2020)
[14] National Digital Department (2019)
[15] Ibid.
[16] Ibid.
[17] PwC (2020)
[18] Ibid.
[19] Economy Planning Unit of Malaysia (2021)

promote digital inclusion, cut service costs and improve efficiency. By the Thirteenth Malaysia Plan (RMK-13), the government confirmed it would serve as the single authentication method for federal services. Since its introduction, the institutional arrangements supporting MyDigital ID have continued to evolve as implementation has progressed. Figure 1 summarises the policy and implementation timeline of MyDigital ID.

Figure 1: Timeline of MyDigital ID Policy and Implementation



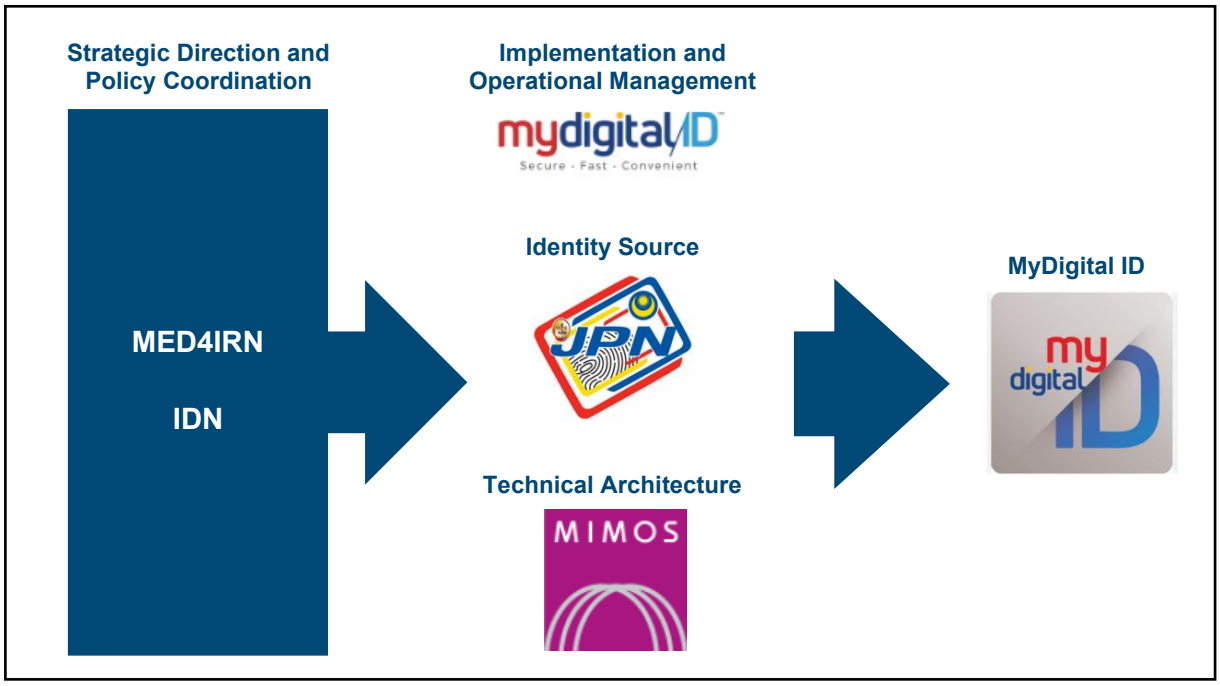
Source: Author's visualisation, compiled from analysis of relevant policy documents

Prior to this, MIMOS Berhad, Malaysia's national applied R&D centre, developed the technological foundation in 2015 and its work was later adopted as the system's architecture[20]. MyDigital ID Sdn. Bhd., incorporated in January 2024 under the Prime Minister's Department, serves as the central implementing agency[21]. The National Registration Department (Jabatan Pendaftaran Negara, JPN) provides authoritative verification by cross-checking enrolments against the national population database[22].

Additionally, the National Digital Economy and Fourth Industrial Revolution Council (MED4IRN), chaired by the Prime Minister, provides strategic oversight of Malaysia's digital identity initiative. This council coordinates digital transformation across the government. Complementing this, the National Digital Identity Council (IDN), chaired by the Minister of Home Affairs, serves as an inter-agency platform to discuss policy directions and strategies related to digital identity initiatives, as well as to monitor programmes linked to national digital identity, such as MyDigital ID. This dual-level coordination structure ensures that MyDigital ID aligns with national digitalisation priorities while maintaining operational focus on identity management and security. Figure 2 maps the institutional roles and oversight relationships that shape the development and implementation of MyDigital ID.

[20] MIMOS Berhad (2026)
[21] MyDigital ID Sdn Bhd (2025)
[22] Ibid.

Figure 2: Institutional Architecture of MyDigital ID



Source: Author's visualisation, based on analysis of multiple policy and institutional sources

Essentially, involving multiple agencies in digital identity is unavoidable, especially when linking it to broader goals, such as the digital transformation of services and the economy or considering it as a foundational DPI. However, ambiguity and conflict arise if the legal and regulatory framework and formal governance structures fail to provide clear institutional mandates and accountability[23]. If roles and relationships are not clearly established and managed, these ministries, agencies and councils could easily generate friction over authority, budgeting and project scope[24].

1.4. Research Objectives and Questions

Building on this context, the discussion paper has three core objectives. First, it examines the key determinants that shape the effectiveness of national digital identity systems, drawing on international frameworks and lessons from established country experiences. Second, it evaluates Malaysia's MyDigital ID against these determinants, analysing its current scope, governance arrangements and inclusivity. Third, it identifies strategic policy measures to strengthen implementation and guide MyDigital ID's evolution into a trusted, rights-based and sustainable digital identity ecosystem.

[23] UNDP (2023b)
[24] Ibid.

The research is guided by three questions:

1. What factors contribute to the effective implementation of national digital identity systems, as reflected in international frameworks and global best practices?

2. What challenges and risks may arise in the implementation of MyDigital ID based on the factors?

3. What policy and institutional improvements can optimise MyDigital ID's implementation to ensure inclusive, trusted and sustainable outcomes?

1.5. Methodology and Approach

This study uses a qualitative, comparative policy analysis approach to examine the effectiveness, challenges and improvement of national digital identity implementation, with a specific focus on Malaysia's MyDigital ID. A qualitative design is suitable because the study aims to understand institutional, governance and socio-technical factors rather than measure quantitative relationships.

The analysis relies mainly on documentary and thematic review of secondary data from policy publications, official government websites, legislative texts, academic literature and reputable media. Insights from stakeholder interviews are also included. Using different sources allows the study to cross-check information and capture both official policy intentions and public discussions on digital identity governance.

A comparative perspective is used to draw policy lessons and identify the structural factors that influence implementation. The analysis looks for patterns, enabling conditions and challenges across countries with digital identity systems. Information is coded along key dimensions such as institutional design, governance arrangements, technology architecture, privacy and data protection, citizen trust and implementation capacity.

The study applies a two-part analytical structure, comprising a conceptual framework and an analytical framework. The conceptual framework defines the main dimensions of an effective digital identity system, based on guidance from recognised international organisations and the digital government literature. These dimensions describe what makes a system credible, secure and trusted. The analytical framework translates these dimensions into practical determinants that can be used to assess both international examples and Malaysia's MyDigital ID.

Taken together, the two frameworks offer a clear way to understand what matters and how to measure effectiveness. This combined approach connects system design and institutional capacity with citizen trust and legitimacy. It supports a comprehensive evaluation of Malaysia's digital identity ecosystem and provides evidence-based recommendations to improve its design, implementation and governance maturity.

2. Framework of Analysis

2.1. Rationale for Selecting International Frameworks

To evaluate the effectiveness of national digital identity systems, it's crucial to anchor the analysis in well-established, globally recognised frameworks. This study explores four key organisations: the World Bank, the United Nations (UN), the Organisation for Economic Co-operation and Development (OECD) and the World Economic Forum (WEF). Each of these organisations has a unique role that adds to this collective framework.

1. World Bank

The World Bank establishes a strong foundation for development and infrastructure through two key initiatives: Identification for Development (ID4D) and DPI. The ID4D program[25] articulates essential principles such as inclusion, design and governance, which are vital for creating effective digital identity systems. It also provides diagnostic tools like the ID4D Global Dataset[26], which assesses important factors such as coverage, accuracy and institutional maturity.

ID4D also outlines ten principles for sustainable identification systems that promote universal coverage, accessibility and the removal of barriers[27]. These principles advocate for robust, secure, and interoperable systems based on open standards, as well as clear institutional mandates with independent oversight and grievance redress. The Practitioners' Guide translates these principles into a life-cycle model encompassing registration, issuance, use, and management, while focusing on deduplication, privacy-by-design and sustainability[28].

In contrast, the DPI framework connects digital identity to broader national digital ecosystems, emphasising its role in ensuring compatibility and functionality across payments, registries and service delivery[29]. This connection is crucial for maximising social value and achieving successful digital identity implementation.

Building on this foundation, the DPI framework positions digital identity as one of three essential public infrastructures, alongside payments and data exchange. It defines identity as a people-centred, safe and interoperable platform that facilitates trustworthy access to digital services and economic participation. By embedding digital identity within a larger interoperability ecosystem, the DPI approach complements ID4D and supports national digital transformation.

[25] World Bank (2019); Clark and Daly (2019); World Bank (2018c)
[26] World Bank (2021b); (2019)
[27] Clark and Daly (2019); World Bank (2019)
[28] Ibid.
[29] World Bank (2025b)

2. UN

The UN, through agencies such as the UN Development Programme (UNDP) and the UN Capital Development Fund (UNCDF), adopts a rights-based and development-oriented approach to digital identity[30]. They view digital identity as an essential public good for achieving Sustainable Development Goal 16.9, which aims for "legal identity for all." This view underscores the need for integrating legal safeguards, inclusion policies and governance frameworks. For the UN, digital identity transcends mere technical infrastructure; it serves as a vital tool for upholding human rights and promoting social empowerment.

The UNDP Model Governance Framework for Digital Legal Identity Systems[31] outlines a rights-based architecture focused on equality, accountability, transparency and the rule of law. It specifies essential governance safeguards, including legal authority, data protection frameworks, independent oversight and accessible grievance redress mechanisms. The UNCDF policy brief links identity to digital financial inclusion, highlighting the importance of affordability, consumer protection and trust in electronic transactions[32].

The report "From Access to Empowerment – Digital Inclusion In A Dynamic World" broadens the concept of inclusion to include digital literacy and multi-channel enrolment, cautioning that access alone does not equal empowerment[33]. Meanwhile, "Accelerating the SDGs through DPI" positions digital identity as a fundamental component of DPI, crucial for achieving Sustainable Development Goal 16.9 and facilitating participation in the digital economy[34]. Collectively, these reports present digital identity as a governance mechanism, a catalyst for development, and a fundamental human right.

3. OECD

The OECD emphasises policy and regulatory issues, aiming to transform technical standards into governance and interoperability guidance for governments and international bodies, such as the G7 and G20. Its analyses draw on comparative experiences from various countries, illustrating how different nations establish consistent Levels of Assurance (LoA), implement privacy-by-design principles and ensure institutional accountability to build cross-border trust.

The OECD views digital identity as part of a comprehensive public governance system. Its "Recommendation of the Council on the Governance of Digital Identity" advocates for user-centred and inclusive systems grounded in privacy-by-design and international interoperability[35]. The framework introduces LoA, which are structured measures of confidence in identity proofing and authentication aimed at enhancing mutual trust both domestically and internationally.

---

[30] UNDP (2023a); (2023c); UNCDF (2022)
[31] UNDP (2023b)
[32] UNCDF (2022)
[33] UNDP (2024)
[34] UNDP (2023a)
[35] OECD (2023)

Additionally, the "DPI for Digital Governments" positions digital identity as a fundamental aspect of modernising digital governance, calling for coordinated, whole-of-government approaches and effective risk management[36]. Complementary studies, like the "G7 Mapping Exercise of Digital Identity Approaches" and the "G20 Collection of Digital Identity Practices", put these principles into action by showcasing collaboration between identity authorities and data protection regulators, harmonised LoA frameworks and ongoing investment in interoperability[37]. Together, these efforts transition the OECD perspective from theoretical principles to practical implementation.

4. WEF

The WEF adds to this discussion by offering a multi-stakeholder perspective that bridges public sector standardisation with private sector innovation. Their reports revolve around the idea of a digital social contract, emphasising trust, user control and sustainability as central to developing robust digital identity ecosystems.

The WEF links digital identity to the evolving digital era social contract between individuals, institutions and states by conceptualising identity as a cornerstone of the digital economy and a new chapter in the social contract, asserting that trust and user control are prerequisites for sustainable participation[38]. Reports on the "Digital Identity Ecosystems: Unlocking New Value" and "Reimagining Digital ID" translate this vision into operational principles[39]. They identify five features of an effective system: user-centric, trusted, interoperable, public-private and sustainable. The WEF emphasises that viable identity ecosystems require "balanced collaboration that combines innovation, digitisation and regulation," cautioning that technology-driven approaches without governance or offline access risk exclusion.

Despite their differences, the four frameworks share a common vision for effective digital identity governance. They all view digital identity as both infrastructure and an institution that relies on legal authority, administrative capacity and social trust. This integrated view leads to two main insights: it provides the theoretical basis that defines a digital identity system and highlights the factors that contribute to its effectiveness. For Malaysia, using these frameworks ensures that MyDigital ID is evaluated according to internationally recognised guidelines, aligning the development with global best practices and boosting public confidence by ensuring the system respects rights, promotes equity and builds trust.

[36] OECD (2024c)
[37] OECD (2024b); (2021)
[38] WEF (2018)
[39] WEF (2023); (2021)

2.2. Deriving Conceptual Dimensions and Analytical Determinants

Conceptual Dimensions

Across these frameworks, four consistent dimensions emerge that together define the structure of an effective digital identity system:

1. Foundational Processes

These are the technical and procedural mechanisms through which identity is created and maintained. The four frameworks describe digital identity as a continuous lifecycle that includes registration, credential issuance, authentication, and ongoing management through updates and revocation40. Data integrity at this stage is crucial because registration errors spread through the system, undermining both accuracy and public trust[41]. Within the OECD and the World Bank's frameworks, Level of Assurance (LoA) such as low, medium or high provides a structured method for determining the confidence level of identity proofing and authentication, guiding how much trust can be placed in a credential[42]. These processes are guided by the principles of accuracy, privacy-by-design and universal accessibility[43]. The WEF emphasised that identity design must start with privacy, security and user control, connecting technical assurance directly to ethical design[44]. Together, these approaches establish the technical credibility of identity as the foundation of its legitimacy.

2. Functional Operations

Once an identity is established, its functionality determines its value. Effective systems allow repeated authentication and verification across multiple services, both online and offline[45]. Open standards, Application Programming Interfaces (APIs), and interoperability frameworks enable portability and cross-sectoral recognition[46]. The OECD underscores interoperability as essential for efficiency and user convenience[47], while the UN and World Bank frameworks highlight integration with payments and data-exchange platforms with secure digital transactions as a defining feature of inclusive digital ecosystems[48]. The WEF describes identity functionality that can be reused securely across contexts without compromising privacy[49]. MyDigital ID is currently operating as an SSO authentication layer, exemplifying an early-stage system that can evolve toward this higher-order interoperability.

---

[40] World Bank (2018c); (2016)
[41] World Bank (2019); (2016); OECD (2011)
[42] OECD (2024b); (2023); World Bank (2016)
[43] World Bank (2019); Clark and Daly (2019)
[44] WEF (2023)
[45] WEF (2021)
[46] World Bank (2019)
[47] OECD (2024c)
[48] World Bank (2025b); UNDP (2023a)
[49] WEF (2021); (2016)

3. Governance and Safeguards

Governance structures establish the legitimacy and accountability of digital identity systems. Effective governance combines clear legal authority, independent oversight, cybersecurity standards and transparent data management. The UNDP identifies accountability, rule of law, equality and transparency as foundational governance pillars, requiring that oversight bodies be legally mandated and publicly accountable[50]. The World Bank and OECD similarly call for privacy-by-default approaches and explicit institutional responsibility for oversight and redress[51]. Additionally, the World Bank emphasizes that trust frameworks and a clear division of responsibilities are essential for sustainable collaboration between public and private sector actors[52]. Governance plays a crucial role in turning identity systems from mere technical tools into trustworthy institutions.

4. Inclusive Design Models

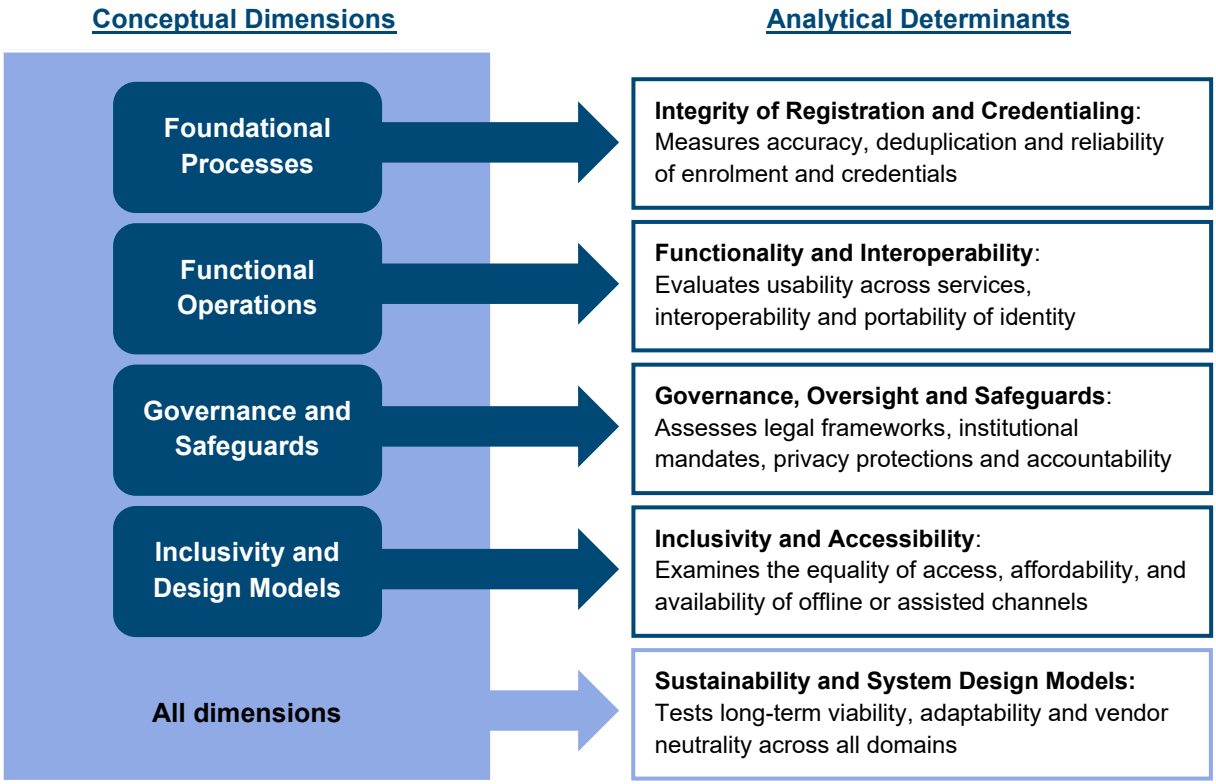
The inclusivity of a digital identity system determines its fairness and reach. Systems must overcome social, economic and infrastructural barriers to ensure that all individuals can enrol and use their credentials. The UNDP emphasises that digital systems should be designed to be rights-based and inclusive from the outset with inclusion going beyond mere access to also include literacy, affordability and participation[53]. The World Bank's inclusive digital identity design demands universal coverage, minimal access barriers, adaptable identity verification, and sustainability via open standards and technology neutrality[54]. The OECD highlights that inclusive digital identity systems must reduce barriers by prioritising accessibility and equity, protecting access for vulnerable groups, preserving non-digital alternatives for essential services, ensuring portability across devices and connectivity conditions and providing adequate user support and skills development[55]. The WEF emphasises that inclusive digital identity systems should provide multiple and accessible enrolment pathways, operate under low connectivity, minimise data disclosure, promote social and financial inclusion, and protect users through robust consent and privacy safeguards[56]. Therefore, inclusivity functions not only as a policy objective but also as an indicator of trust and system legitimacy.

[50] UNDP (2023b); (2023a)
[51] OECD (2023); World Bank (2019)
[52] World Bank (2016)
[53] UNDP (2024); (2023b)
[54] World Bank (2019); (2018c); (2016)
[55] OECD (2023)
[56] WEF (2023); (2018)

Analytical Determinants

These frameworks also identify key analytical determinants that translate conceptual dimensions into practical applications. While the dimensions provide a structural foundation, these determinants evaluate the quality of outcomes. For clarity, the relationship between the four conceptual dimensions and the five analytical determinants is summarised in Figure 3:

Figure 3: Relationship between Conceptual Dimensions and Analytical Determinants of Digital Identity Effectiveness



Source: Author's visualisation, synthesised from digital identity frameworks by the World Bank, UN, OECD and WEF

1. Integrity of Registration and Credentialing

Integrity ensures that each enrolled identity is uniquely matched to a real person. Across various frameworks, there is a strong consensus that trusted digital identity systems rely on high integrity during registration and credentialing. This relies on rigorous identity proofing, accurate and current attributes, effective deduplication often supported by biometrics, and reliable authentication to establish appropriate levels of assurance and trust. Organisations differ in emphasis, with the World Bank mainly framing integrity in terms of development value and operational confidence through levels of assurance[57], while UN frameworks focus on legal reliability and compliance with international standards[58], the OECD highlighting governance,

[57] World Bank (2019); (2018c); (2016)
[58] United Nations (2022); UNCDF (2022)

authoritative data sources and proportionality to reduce fraud while protecting privacy[59], and the WEF emphasising system fitness for purpose, ongoing reliability and the benefits of high assurance identity for relying parties[60]. For an SSO-based system, integrity depends on reliable electronic Know Your Customer (eKYC) procedures, biometric cross-checks with national registries and mechanisms for periodic data validation.

2. Functionality and Interoperability

A digital identity system creates value only when it can be used easily and securely across services. The frameworks emphasise that effective digital identity systems must be functional, usable, and interoperable to expand access to services, support innovation, and deliver value across public and private sectors with portability and open standards seen as essential for scaling, efficiency and building user trust. The World Bank focuses on functionality, interoperability and portability as design principles to enhance service delivery efficiency and enable innovation across sectors[61], while the UN frames these elements within DPI to democratise access, incorporate human-centred design and support cross-sector and cross-border use[62]. The OECD prioritises governance, usability and portability across platforms, sectors, and jurisdictions through trust frameworks and standards to facilitate public-private collaboration[63], and WEF stresses operational effectiveness, user experience and value creation through interoperable and portable identity systems, while warning that increased connectivity must be carefully managed to reduce security risks[64].

3. Governance, Oversight and Safeguards

Across the four organisations, there is broad convergence that effective digital identity systems depend on strong governance arrangements, including clear institutional mandates, coherent legal frameworks, independent oversight, enforceable accountability, and grievance redress mechanisms, as well as privacy and security safeguards embedded by design. The World Bank views governance as a prerequisite for inclusion, efficiency and development impact[65], the UN is placing greater weight on rights-based governance, the rule of law and legally enforceable liability[66], the OECD focuses on strategic stewardship, policy coherence, proportional risk management and long-term sustainability[67], and the WEF emphasising user-centric governance, public–private collaboration, flexible oversight models and enhanced individual control over personal data[68].

[59] OECD (2023); (2024b)
[60] WEF (2023); (2018)
[61] World Bank (2019); (2018c); (2016); Dahan and Sudan (2015)
[62] UNDP (2024); (2023a); United Nations (2022); UNCDF (2022)
[63] OECD (2023); (2021)
[64] WEF (2021); (2018); (2016)
[65] World Bank (2019); (2018c); (2016); Dahan and Sudan (2015)
[66] UNDP (2023b); (2023a); United Nations (2022); UNCDF (2022)
[67] OECD (2023); (2021)
[68] WEF (2023); (2021); (2018); (2016)

4. Inclusivity and Accessibility

All four organisations emphasise universal and non-discriminatory coverage across the life course, the need to actively remove access and affordability barriers, and the importance of ensuring that vulnerable groups such as the poor, rural populations, women, persons with disabilities, migrants and those with low digital literacy are not excluded. Each framework also stresses the necessity of offline, assisted or multi-modal access channels to address connectivity constraints and last-mile challenges, and recognises affordability as critical, particularly by discouraging fees for initial registration and core identity credentials. They differ mainly in emphasis, as explained under the conceptual dimension above, with the World Bank framing inclusion through a development and service-delivery lens, the UN grounding it in rights-based equality and DPI principles, the OECD treating inclusivity as a governance obligation that requires preserving non-digital alternatives and assisted access, and the WEF emphasising inclusivity as a defining system quality that relies on multiple entry points, minimal data disclosure, affordable models, and strong links to financial and social inclusion.

5. Sustainability and System Design Models

Sustainable digital identity systems must be designed for long-term viability, adaptability and vendor neutrality, with open standards, modular architectures and avoidance of vendor lock-in viewed as essential to resilience, affordability and innovation. All four organisations highlight the importance of sound financial and governance models, flexibility to adapt to technological and policy change, and system designs that can scale and evolve over time without compromising access or sovereignty. The World Bank focuses on sustainability as a design principle linked to development impact, financial planning and procurement discipline[69], the UN framing sustainability and adaptability within DPI and legal principles such as technological neutrality and cross-domain applicability for achieving the SDGs[70], the OECD approaching sustainability through strategic governance, long-term investment, market shaping and prevention of dependency risks on single vendor[71], and the WEF highlighting system viability through stakeholder value, operational resilience, flexible funding models and the need to manage vendor neutrality to support user-centric and interoperable identity ecosystems[72].

[69] World Bank (2025b); (2019); (2016); Dahan and Sudan (2015)
[70] UNDP (2023a); (2023b); United Nations (2022)
[71] OECD (2024c); (2023)
[72] WEF (2021); (2018); (2016)

2.3. Analytical Framework for Evaluation

The five analytical determinants create a structured evaluation framework that helps translate guidance from organisations like the World Bank, UNDP, OECD and WEF into a practical diagnostic tool for digital identity systems, regardless of their maturity level. This framework is designed to ensure that assessments are both systematic and fair, enabling even entry level systems, like Malaysia's MyDigital ID which functions as an SSO authentication platform to be evaluated alongside more advanced infrastructures found in countries like Estonia, Singapore or India. The goal is not to rank these systems but to pinpoint their progress, identify existing gaps and explore viable pathways for development within a unified evaluative structure.

The framework recognises that digital identity systems develop gradually. In the initial phase, identity systems mainly serve authentication functions like SSO[73]; at the intermediate phase they achieve interoperability across agencies[74]; and at the advanced phase, they operate as foundational infrastructures integrating identity with payments, registries and data exchange[75]. For this analysis, the intermediate and advanced phases are treated as a single developmental stage following the initial SSO phase, because leading international frameworks indicate that cross-agency interoperability and the progression toward foundational digital infrastructures rest on the same technical and governance foundations.

OECD underscores that both developments require shared governance mechanisms and common technical standards established after the authentication[76], UN highlights that these capabilities depend on open, extensible architectures and accountable governance necessary to move beyond single-purpose systems[77], WEF similarly emphasises the need for an attribute-exchange layer and mutually accepted governance arrangements to support trusted transactions at scale[78], and the World Bank observes that both elements rely on core architectural building blocks and comprehensive governance frameworks that enable digital identity to operate as part of a wider digital public infrastructure[79].

The analytical framework assumes that for instance, achieving interoperability without strong governance could improve service delivery but undermine privacy, while advanced technology without inclusive access could deepen inequality.

[73] OECD (2024c); WEF (2021); (2016); World Bank (2019); (2018c)
[74] OECD (2024c); UNDP (2023a); (2023b); WEF (2021); World Bank (2023); (2019); (2018c)
[75] OECD (2024c); UNDP (2024); (2023a); WEF (2019); (2018); World Bank (2025b); (2023)
[76] OECD (2023)
[77] UNDP (2023a); United Nations (2022)
[78] WEF (2018); (2021)
[79] World Bank (2025b)

Figure 4: Analytical Framework for Evaluating Digital Identity Systems

Analytical Determinants	Core Elements	Application Across System Maturity
Integrity of Registration and Credentialing	Accuracy and validation, deduplication and uniqueness, and reliability of credentials	SSO: eKYC and biometric validation Foundational: Lifecycle registration and continuous update
Functionality and Interoperability	Usability across services, interoperability and portability	SSO: Confined to public portals Foundational: Linked to payments, registries and cross-border transactions
Governance, Oversight and Safeguards	Governance and institutional mandates, legal frameworks and oversight, and privacy protection and safeguards	SSO: Single-agency oversight Foundational: Multi-agency and independent supervision
Inclusivity and Accessibility	Equality of access and non-discrimination, affordability, and availability of offline or assisted channels	SSO: Connectivity and device limits Foundational: Universal access with targeted support
Sustainability and System Design Models	Long-term viability and sustainability, adaptability and resilience, and vendor neutrality and openness	SSO: Pilot-stage sustainability Foundational: Stable funding and federated/decentralised architecture

Source: Author's table, synthesised from digital identity frameworks by the World Bank, UN, OECD and WEF

Figure 4 illustrates how the five analytical determinants operate across different stages of digital identity maturity from SSO to foundational digital infrastructures. The application of this framework proceeds by applying it to:

- international case studies (Estonia, Singapore and India) to illustrate implementation pathways and identify transferable lessons; and
- Malaysia's MyDigital ID, evaluating its current performance and alignment with global benchmarks.

This ensures that subsequent analysis is consistent and directly linked to the determinants.

3. International Best Practices and Case Studies

This section explores five analytical determinants that contribute to the effectiveness of the selected international digital identity systems. The goal is to examine how established digital identity ecosystems apply these factors and how their experiences can offer valuable insights for Malaysia's MyDigital ID initiative. This analysis draws on data from reputable international organisations such as the World Bank, OECD, UN and WEF, as well as official government and reliable sources.

Estonia, Singapore and India were chosen because they represent a wide range of governance styles, technological advancement levels and developmental situations. Together, they showcase different approaches to implementing national digital identities and provide valuable insights based on the five analytical determinants.

3.1. Estonia

Estonia's digital identity system represents one of the world's most comprehensive integrations of legal identity, data exchange and public-service delivery. After regaining independence in 1991, the government built a unified population register and an electronic identification framework that now underpin nearly all digital transactions across public and private sectors[80]. The system demonstrates how coherent legal, technical and institutional design operationalises all five determinants of effective implementation.

The **integrity of registration and credentialing** is anchored in the Population Register as the single authoritative source of identity data, ensuring accurate and timely civil registration, preventing duplication across government systems, and enabling cross-validation through a unique Personal Identification Code (PIC) assigned at birth[81]. Uniqueness is enforced through a civil-registry-based, non-biometric model that maintains one record per person, while high levels of assurance are achieved through mandatory chip-based electronic ID credentials that support strong authentication and legally binding digital signatures[82]. The Police and Border Guard Board issues and manages identity credentials, ensuring deduplication and secure lifecycle management under the Ministry of the Interior[83].

Functionality and interoperability are achieved by operating as a cross-sector platform that offers near-universal online access to public and private services through mandatory high-assurance credentials[84], including the ID-card (chip-based), Mobile-ID (SIM-based for smartphones) and Smart-ID (app-based authentication)[85]. Currently, 19% of Estonians use Mobile ID[86] and 53% use Smart ID[87]. Strong usability and trust are supported by legally binding digital signatures recognised at the highest level under European Union (EU) law, enabling

[80] World Bank (2015)
[81] Ibid.
[82] World Bank (2015)
[83] Ibid.
[84] World Bank (2015); (2014); Estonian Business and Innovation Agency (2025a)
[85] Estonian Business and Innovation Agency (2025a)
[86] Estonian Business and Innovation Agency (2025b)
[87] Estonian Business and Innovation Agency (2025c)

efficient, high-value transactions across sectors such as healthcare, banking, business and e-government[88].

Interoperability is achieved through a decentralised architecture anchored in a single PIC and the X-tee data exchange layer (also known as "X-Road"), which enables secure, standardised and auditable data sharing while avoiding centralised data storage[89]. This design also ensures high portability across devices, services and borders, reinforced by compliance with the EU eIDAS (electronic Identification, Authentication and Trust Services) framework, cross-border data exchange with neighbouring states and the e-Residency programme, positioning Estonia's digital identity as a lifetime, cross-platform and internationally interoperable credential[90]. The X-tee now supports approximately 52,000 organisations as indirect users, processes 2.2 billion transactions annually and enables over 3,000 e-services[91]. Each agency retains ownership of its data; only encrypted requests traverse X-tee, preventing centralised storage[92].

Governance, oversight and safeguards are built into a clear framework of legal, institutional and technical measures that maintain accountability and public trust through strong political support, decentralised data management and explicit institutional responsibilities. Governance responsibilities are clearly allocated across the Ministry of the Interior, the Police and Border Guard Board and the Estonian Information System Authority (RIA) that administers trust and cybersecurity frameworks, with transparency reinforced through a national registry of public information systems[93].

Cyber-resilience has become increasingly important, with a total of 6,515 cyber incidents impacting organisations in 2024, almost doubling the number from 2023 including 4,224 phishing and scam cases and 637 service disruptions[94]. RIA publicly reported major authentication service interruptions in March and September 2024, caused by large-scale DDoS attacks[95]. This transparency, along with the activation of a national cyber reserve, illustrates Estonia's mature oversight ecosystem. The RIA's unique cyber reserve is a team composed of experts from RIA, other state IT agencies, and the Estonian Defence League's Cyber Unit, which is deployed when a cyber incident severely disrupts a critical service, and the affected organisation cannot resolve the situation swiftly[96].

The legal framework ensures personal data protection as a constitutional right, supported by independent oversight from the Estonian Data Protection Inspectorate and enforceable accountability mechanisms that allow citizens to view access logs and seek redress for misuse[97]. Privacy and security are embedded by design through data minimisation, the once-only principle,

[88] World Bank (2015); (2014); Estonian Business and Innovation Agency (2025c)
[89] World Bank (2015); Nortal (2025)
[90] World Bank (2015); Estonian Business and Innovation Agency (2025a)
[91] Estonian Business and Innovation Agency (2024)
[92] World Bank (2018a)
[93] World Bank (2015)
[94] Information System Authority (RIA) (2025a)
[95] Information System Authority (RIA) (2024a); (2024b)
[96] Information System Authority (RIA) (2025a)
[97] World Bank (2018a); (2015)

user control over data access and a secure X-tee exchange layer that relies on encryption, time stamping and tamper-proof digital logs to ensure integrity across the digital identity ecosystem[98].

Inclusivity and accessibility remain defining features. Legal identity is established at birth through the automatic assignment of a PIC, while mandatory e- ID for residents over 15 ensures near-universal coverage and equal access to public services, including the automatic linkage of birth registration to health insurance entitlements[99]. Mandatory inclusion led to over 99% of residents obtaining an electronic identity (e-ID)[100]. Estonia's high internet connectivity, digital literacy initiatives including targeted training programmes for older participants and face-to-face cybersecurity awareness workshops, multiple digital credentials, and widespread service support ensure equitable participation[101]. To broaden reach, the RIA launched the Eesti app, a mobile portal consolidating more than 50 public services[102]. In June 2025, Parliament authorised the app to serve as a legal identity tool via QR-code or barcode verification once users authenticate through e-ID, Smart-ID or EU eID[103]. This diversification of modalities enhances inclusion and convenience.

Sustainability and system design in Estonia rest on a cost-effective public funding model and stable operational arrangements. System adaptability is enabled by a modular and decentralised architecture centred on the X-tee data exchange platform, which allows for scalable participation, continuous technological upgrading, and strong cyber resilience through encryption, time stamping and ongoing security assessment[104]. Sustainability is further reinforced through adherence to open standards, open-source components, and technology and vendor neutrality, which prevent lock in and support competition, while regulated public-private partnerships allow selected components to be outsourced without weakening state control over core identity infrastructure[105]. Core components, including X tee, are open source and maintained by the Nordic Institute for Interoperability Solutions[106]. Together, these arrangements demonstrate institutional continuity and adaptive sustainability in a high-trust governance environment.

Estonia demonstrates how integrity, interoperability, governance, inclusivity and sustainability reinforce each other within a mature foundational-identity ecosystem. The expansion of X-tee, the adoption of a legally recognised mobile identity and transparent cyber-governance confirm that durability arises from continual institutional adaptation rather than static design. For Malaysia, Estonia's trajectory underscores that progressing from SSO authentication to foundational identity requires parallel investments in legal clarity, interoperable architecture, inclusive access channels and accountable oversight.

[98] World Bank (2015); (2014); Nortal (2025)
[99] World Bank (2015)
[100] Estonian Business and Innovation Agency (2025a)
[101] World Bank (2015); Estonian Business and Innovation Agency (2025a); Information System Authority (RIA) (2025a)
[102] Information System Authority (RIA) (2025c)
[103] Information System Authority (2025)
[104] World Bank (2015); Nordic Institute for Interoperability Solutions (2025); Nortal (2025)
[105] World Bank (2016); (2015); (2014); Nortal (2025); Nordic Institute for Interoperability Solutions (2025)
[106] Nordic Institute for Interoperability Solutions (2025)

3.2. Singapore

Introduced in 2003, Singapore's Singpass has evolved from a basic authentication portal into a core national digital identity platform[107]. MyInfo, launched in 2016, extends its functionality by enabling consent-based data sharing across public and private services[108]. Singapore's national digital identity[109] is described as a secure authentication system that enables individuals to access government and business e-services, with policy and operational coordination anchored in Smart Nation initiatives and the Government Technology Agency's (GovTech) delivery capabilities. Singapore's architecture links authentication with consent-based personal data provision through Singpass and MyInfo, which are presented as core instruments for streamlining transactions while maintaining data protection and auditability across agencies and regulated private sector use cases. This model illustrates how a state-led trust framework supports cross-sector reuse of authoritative attributes via APIs and standardised onboarding, while retaining role clarity for policy, cybersecurity and service delivery.

Integrity of registration and credentialing is sustained through validation against authoritative registries, with Singpass used to verify identity for access to e-government services and for corporate transactions via Corppass, the corporate authorisation framework that enables organisations to access government and public-service digital platforms. Personal data flows from government sources to relying parties under explicit user consent, and MyInfo is positioned as a platform that pre-fills verified data to reduce manual entry and error, while MyInfo Business and its APIs similarly enable an authorised officer to consent to sharing verified corporate data for government-to-business transactions.

Building on this architecture, Singpass achieves high integrity and assurance by leveraging a universally issued foundational ID system, authoritative "single sources of truth" managed by agencies such as Immigration and Checkpoints Authority (ICA) and Inland Revenue Authority of Singapore, biometric deduplication linked to mandatory national identifiers, and strong authentication mechanisms. Reliability is further reinforced through high-assurance identity proofing, multi-factor authentication, PKI-based credentials, legally recognised digital signatures, adherence to open authentication standards and continuous security monitoring under clear legal and governance frameworks, enabling Singpass to function as a trusted and auditable national authentication layer.

[107] World Bank (2022); OECD (2021)

[108] Ibid.

[109] All information related to Singpass is obtained from the Case Study Report on National Digital Identity and Government Data Sharing in Singapore - A Case Study of Singpass and APEX 2022 [World Bank (2022)], unless stated otherwise

Functionality and interoperability are organised through API-based integration patterns and a developer ecosystem that supports secure identity, data sharing and digital signatures ("Sign with Singpass"), enabling reuse across government and regulated commercial domains[110]. A structured specification set documents interfaces, authorisation sequences and test–production environments that facilitate consistent onboarding of relying parties, while a progressive security upgrade for authentication interfaces aims to comply with financial-grade API profiles supported by clear migration guidance[111]. These reinforce the positioning of Singpass and MyInfo as core levers for seamless cross-agency service delivery and private-sector participation under common technical standards[112].

Building on this foundation, Singapore's national digital identity ecosystem, centred on Singpass and supported by MyInfo and the APEX data exchange platform, demonstrates strong functionality, usability and interoperability through widespread adoption, user-centric design and extensive cross-sector integration. Singpass enables access to thousands of public and private services with appropriate levels of assurance, while MyInfo streamlines transactions through consent-based data sharing from authoritative government sources, and APEX underpins secure, standardised API-based data exchange across government and business systems, positioning Singapore's NDI as a scalable and trusted foundation for digital service delivery.

Governance, oversight and safeguards are articulated through institutional arrangements that assign system development and operations to GovTech and policy coordination to Smart Nation bodies, with national cybersecurity authorities providing assurance functions[113], while MyInfo transactions are governed by explicit consent, authorised use and audit requirements that clarify user-permissioned pre-filling and the obligations of relying parties. Corppass further reinforces layered assurance by requiring business users to first verify their identity through Singpass before accessing government digital services, embedding organisational accountability within the identity framework.

Based on these arrangements, Singapore's digital identity ecosystem, centred on Singpass and the APEX data exchange platform, is characterised by strong central governance, clear institutional mandates and comprehensive legal and technical safeguards anchored in long-term political commitment under the Smart Nation initiative. Governance responsibilities are clearly delineated supported by a layered legal framework covering data governance, electronic transactions and cybersecurity, and reinforced by consent-based data sharing, data minimisation and real-time security monitoring, while ongoing debate over the exclusion of public sector agencies from core provisions of the Personal Data Protection Act 2012 highlights tensions between centralised state control and public expectations of transparency and privacy protection[114].

[110] World Bank (2022); Singpass (2025)
[111] World Bank (2022); Cyber Security Agency of Singapore (2021)
[112] World Bank (2022); Smart Nation Singapore (2024)
[113] World Bank (2022); Cyber Security Agency of Singapore (2021)
[114] Personal Data Protection Commission (PDPC) (2022); Teo and Harjani (2021)

Inclusivity and accessibility are framed in Smart Nation materials[115] as part of a broader approach to improve digital access, literacy and adoption, with Singpass was introduced to provide a single login to a wide range of government e-services to deliver faster and more personalised services while maintaining a consistent, citizen-facing interface for essential transactions. Accessibility is reinforced through inclusive design practices, multilingual support, coverage of both citizens and migrant residents, and free access to digital credentials delivered via widely owned mobile devices. Affordability is further strengthened through targeted subsidies for broadband, devices and mobile access for low-income households and seniors, while multiple offline and assisted options, including community-based support counters, physical service centres, alternative verification methods and nationwide digital literacy programmes, help mitigate digital exclusion for individuals unable or unwilling to rely solely on digital channels.

Sustainability and system design are presented as iterative and adaptive, with Smart Nation outlining a phased vision that spans from initial national digital projects to a refreshed framework, positioning digital identity as a continuing strategic priority. Developer updates further describe a proactive security roadmap for authentication APIs, emphasising ongoing maintenance and progressively higher assurance profiles, while government guidance highlights platform stewardship, component reuse within a unified technology stack and sustained support for secure, standardised integration. The system's resilience is reinforced by an evolutionary, modular design that enables continuous technological upgrades, scalable cloud deployment and rapid service development through shared government technology components and a central data exchange platform. Sustainability is further strengthened by adherence to open standards, growing in-house development capabilities and open developer access, which together reduce vendor dependency, prevent lock-in and ensure that the digital identity infrastructure remains flexible, interoperable and responsive to future technological and security challenges.

3.3. India

India's national digital identity system functions as a foundational framework centred on Aadhaar, administered by the Unique Identification Authority of India (UIDAI) under the statutory Aadhaar Act of 2016 for authentication[116]. It links biometric enrolment and deduplication to ensure uniqueness and provides an authentication infrastructure supporting welfare delivery, financial inclusion and regulatory compliance[117]. In parallel, the Ayushman Bharat Digital Mission (ABDM) establishes a federated health-information ecosystem based on open standards, registries, and consented data exchange, extending the reach of digital identity into sectoral platforms[118]. Together, these initiatives define a large-scale foundational identity oriented toward inclusion, interoperability and institutional safeguards.

[115] World Bank (2022); Smart Nation Singapore (2024)
[116] Banerjee (2016); World Bank (2014); NEXT IAS (2025)
[117] World Bank (2018a); (2014); Republic of India (2016)
[118] World Bank (2025a)

The integrity of registration and credentialing in India's Aadhaar system is achieved through biometric capture, large-scale deduplication and the unique lifetime assignment of Aadhaar numbers, establishing a reliable basis for authentication across services[119]. As a foundational digital identity covering about 1.24 billion residents by mid-2022[120], Aadhaar supports accuracy through the collection of demographic attributes combined with multimodal biometrics, strict statutory limits on sensitive data collection, central verification by UIDAI and mechanisms for updating records over time[121]. Uniqueness is ensured through extensive biometric deduplication and a randomly generated, persistent identifier, while reliability is maintained through cloud-based authentication utilising demographic or biometric factors, along with mandated fallback mechanisms in the event of authentication failure[122].

Privacy-by-design features such as Virtual ID and tokenisation minimise exposure of the Aadhaar number and enable temporary, revocable identifiers for authorised use[123], and integrity is reinforced through multiple authentication modalities including fingerprint, iris and face, supported by UIDAI's authentication infrastructure[124]. Official data indicate that Aadhaar face-authentication transactions exceeded 100 crore (1 billion transactions) in Financial Year 2024 to 2025, while monthly totals of all authentications exceeded 220 crore (2.2 billion transactions) by mid-2025, reflecting sustained growth in verified usage and demonstrating both operational reliability and public adoption[125]. At the same time, despite strong architectural safeguards and judicially imposed limits on data retention[126], past incidents of credential misuse and access control failures have highlighted vulnerabilities in governance and oversight rather than in the biometric core itself[127].

Functionality and interoperability in India's Aadhaar system are realised through Aadhaar-enabled e-KYC and authentication services integrated across banking, telecom, payments, welfare and health systems, positioning Aadhaar as a foundational digital identity infrastructure that enables remote authentication and large-scale service delivery[128]. The digital identity toolkit highlights Aadhaar e-KYC as a mechanism enabling paperless onboarding and remote verification[129], while UIDAI's online and paperless-offline e-KYC allows residents to verify identity through digitally signed, user-controlled XML documents[130], significantly reducing onboarding costs and enabling high-volume transactions[131]. Interoperability is achieved through a unique lifetime, persistent identifier[132] and open APIs under IndiaStack, which support

[119] World Bank (2021a)
[120] World Bank (2025a); (2021a)
[121] World Bank (2018a); (2016); Republic of India (2016)
[122] World Bank (2018a); (2016); (2014); Republic of India (2016)
[123] World Bank (2018a)
[124] World Bank (2018a); (2016); (2014)
[125] Unique Identification Authority of India (UIDAI) (2025a); (2025b)
[126] Republic of India (2016); Supreme Court Observer (2018)
[127] Burgess (2025)
[128] Republic of India (2016); World Bank (2021a); (2018b); Banerjee (2016)
[129] World Bank (2021a); (2016); Banerjee (2016)
[130] World Bank (2023); (2021a); (2018a)
[131] World Bank (2021a); (2018b); Banerjee (2016)
[132] Supreme Court Observer (2018); World Bank (2014)

seamless integration across public and private platforms and underpin major national initiatives[133].

Foundational ID thereby operates as a reusable trust layer connecting individuals to payments and social-benefit delivery while in health, ABDM links the Ayushman Bharat Health Account number with health facility, professional registries and personal health records within a federated, open-API environment that ensures consent-based data exchange[134]. These architectures collectively illustrate an ecosystem in which authentication and interoperability reinforce each other across sectors.

Governance, oversight and safeguards are embedded in statutory and administrative structures that regulate authentication, e-KYC and data-protection practices, operating within a centralised governance framework led by UIDAI[135]. Formalised under the Aadhaar Act 2016, UIDAI is responsible for enrolment, authentication, operation of the central database and grievance redress, while the scope and use of Aadhaar have been shaped by sustained judicial scrutiny, including Supreme Court rulings that upheld constitutionality but imposed limits on mandatory use, private-sector access and data retention[136]. Privacy-preserving instruments such as Virtual ID, tokenisation and granular attribute release translate regulatory principles of data minimisation and purpose limitation into operational mechanisms, complementing consent-based authentication and strict controls on biometric use[137]. The coexistence of a strong legal framework and adaptive administrative control has enabled India to maintain accountability while managing identity infrastructure at a population scale.

Inclusivity and accessibility define India's foundational ID trajectory, reflecting a strong policy commitment to universal inclusion through the provision of a free, portable digital identity for all residents, with specific mandates to reach vulnerable groups such as women, migrant workers, persons with disabilities and unorganised labour[138]. The system covers over 1.2 billion people, facilitating direct benefit transfers, account opening and access to essential services, while affordability is reinforced through free enrolment and a cloud-based model that avoids the cost of physical cards[139]. By reducing KYC costs and enabling remote verification, Aadhaar supports formal-sector participation and private-sector inclusion[140], complemented by assisted enrolment and authentication channels that extend access in low-literacy and low-connectivity settings[141]. Transaction statistics confirm sustained use of Aadhaar authentication for welfare and commercial purposes, with continual growth in biometric and face-based usage. At the same time, reliance on biometric authentication has exposed exclusion risks due to technological failures, prompting legal requirements for alternative identification methods and offline verification, underscoring that inclusivity in Aadhaar is pursued not only through enrolment

[133] World Bank (2021a); (2018b)
[134] World Bank (2025a)
[135] Republic of India (2016); World Bank (2018a)
[136] Republic of India (2016); Supreme Court Observer (2018); World Bank (2018a)
[137] Republic of India (2016); World Bank (2018a)
[138] Banerjee (2016); World Bank (2014)
[139] World Bank (2025a); (2016); Banerjee (2016)
[140] World Bank (2018b)
[141] World Bank (2025a); (2014)

coverage but also through the active, safeguarded use of digital credentials in everyday service access[142].

Sustainability and system design rest on institutional scale, open standards and iterative adaptation, with Aadhaar functioning as a foundational component of India's DPI that links identification, payments and service delivery through interoperable interfaces[143]. Designed for long-term viability through an "identity in the cloud" model, Aadhaar avoids the costs of physical credentials, leverages economies of scale and supports projected fiscal returns by reducing fraud and leakage, even as debates continue over cost recovery and public-good financing[144]. Adaptability is enabled by a persistent lifetime identifier, modular and federated architectures and open APIs, while the ABDM adopts open-API specifications and federated registries to maintain long-term flexibility across health systems[145]. UIDAI's continuous technical updates, including the expansion of face authentication and revisions to e-KYC response formats, demonstrate ongoing maintenance and evolution of the identity stack, alongside privacy-enhancing safeguards such as virtual IDs and tokenisation introduced in response to emerging risks[146]. These features indicate that sustainability in India's model is achieved through large-scale operations anchored in legal mandate, open standards, vendor neutrality and administrative continuity.

India's digital identity system serves as a foundational model that integrates biometric security, interoperable features, regulatory oversight, broad accessibility and flexible sustainability. The Aadhaar platform and sector-specific extensions, such as ABDM, demonstrate how large-scale systems can maintain governance and privacy-by-design principles, creating a foundational identity that supports both inclusion and accountability over time.

3.4. Cross-Country Insights

The development of these systems followed staggered but mostly overlapping paths: Estonia introduced its e-ID in 2002, Singapore launched Singpass in 2003 and later expanded its digital identity features through MyInfo in 2016, while India began Aadhaar enrolment in 2009 followed by statutory consolidation in 2016. These timelines show that although the systems appeared during a similar technological era, their institutional routes diverged in ways that influenced their governance arrangements and maturity.

The evidence drawn from Estonia, Singapore and India demonstrates how different governance structures and development contexts influence the operationalisation of the five determinants of effective digital identity implementation. Each system exhibits internal coherence between legal foundations, institutional design, and technology architecture, yet the pathways taken reflect distinct national priorities: integrated e-governance in Estonia, efficient digital services in Singapore and welfare inclusion in India.

---

[142] Supreme Court Observer (2018); Burgess (2025)
[143] World Bank (2025a); (2014)
[144] Banerjee (2016); World Bank (2014)
[145] World Bank (2025a); (2014)
[146] World Bank (2018a); NEXT IAS (2025)

Integrity of Registration and Credentialing is central across the systems, with shared emphasis on accuracy, uniqueness and assurance, but achieved through context-specific designs. Estonia relies on a civil-registry-based, non-biometric model, Singapore combines authoritative registries with biometric verification and multi-factor authentication, while India prioritises population-scale biometric deduplication and cloud-based, multi-modal authentication.

Functionality and Interoperability underpin all three systems, enabling cross-sector service delivery through interoperable architectures. Estonia emphasises decentralised, standards-based data exchange and cross-border portability, Singapore adopts API-driven, consent-based integration for seamless domestic services, and India uses a persistent identifier and open APIs to operate Aadhaar as a reusable trust layer supporting population-scale authentication and sectoral platforms such as digital health.

Governance, Oversight and Safeguards are foundational across all three systems, with strong state stewardship and legal frameworks supporting trust and accountability. Estonia combines decentralised institutions with constitutional privacy protections, Singapore relies on central executive leadership and consent-based safeguards, while India adopts a statutory, centralised model shaped by judicial oversight and reinforced through operational privacy-preserving mechanisms.

Inclusivity and Accessibility are shared priorities across the three systems, though shaped by different contexts. Estonia benefits from high connectivity and mandatory coverage, Singapore emphasises inclusive design, affordability and assisted access for diverse residents, while India pursues universal, free enrolment at scale, balancing remote verification gains with safeguards to address biometric-related exclusion risks.

Sustainability and System Design Models reflect shared commitments to longevity, modularity and open standards across all three systems. Estonia highlights decentralised, cost-efficient public infrastructure and strict vendor neutrality, Singapore implements an evolutionary, cloud-ready approach with growing in-house capabilities, and India leverages scale through a cloud-based, federated architecture that enables continuous adaptation while avoiding physical credential costs.

Comparatively, Estonia represents a foundational integrated model grounded in trust and legal precision, Singapore exemplifies a federated, citizen-centric model driven by institutional coordination and iterative design, and India embodies a foundational, high-scale model aimed at universal inclusion within a rights-based framework. All three illustrate that effectiveness stems from alignment between governance and technical systems rather than from technology alone. Where Estonia shows that transparency and decentralised interoperability generate durable trust, Singapore proves that federated governance can deliver efficiency without sacrificing assurance, and India demonstrates that inclusion and rights protection must evolve together to sustain legitimacy at scale.

Viewed time, these cases show that digital identity maturity is path-dependent: early adopters like Estonia took more than twenty years to achieve institutional integration, mid-cycle reformers such as Singapore improved through iterative upgrades, and late but large-scale entrants like India quickly achieved inclusion via statutory consolidation. In all three, institutional alignment

developed gradually rather than at the start, highlighting that maturity results from ongoing legal, technical, and organizational growth rather than a one-time technological implementation.

3.5. Key Comparisons and Constraints

Experience from other countries shows that differences in population, infrastructure, and government capacity shape how digital identity systems work, and explain why MyDigital ID cannot simply copy any single foreign model.

One important point of comparison concerns the foundational identity systems on which digital identity has been built in each country. Estonia and Singapore both built digital identity on top of long-standing universal civil registration systems and mandatory identity cards, which provided a stable base for secure authentication. Singapore similarly anchors Singpass on the National Registration Identity Card (NRIC) system, which has been compulsory for decades and is used throughout public administration. India, by contrast, adopted Aadhaar to address gaps in foundational identity coverage, relying on biometrics as a large-scale enrolment and deduplication mechanism. Malaysia's context aligns more closely with Estonia and Singapore because the JPN maintains a comprehensive population registry and MyKad is universally issued. This means that Malaysia does not need India's biometric-first approach, but it also signals that data-quality issues in the registry would directly affect MyDigital ID unless they are strengthened.

A second point of comparison relates to assumptions about population scale, connectivity and geographic distribution, which shape both system design and implementation risk. Estonia's digital identity architecture was designed for a small, highly connected society with high internet penetration and near-universal use of eID cards. Singapore similarly relies on widespread mobile penetration and consistent broadband availability to support Singpass and its mobile-based authentication. India's Aadhaar model, in contrast, uses cloud-based real-time authentication partly because distributing secure smartcards to over a billion people would have been logistically and financially prohibitive. Malaysia occupies a middle ground. Its population is more geographically dispersed than Estonia and Singapore yet far smaller than India. Connectivity and device disparities across rural regions imply that Malaysia cannot assume continuous online availability or uniform smartphone access. A hybrid model that supports online and offline authentication is therefore more aligned with Malaysia's demographic and infrastructural profile, consistent with international recommendations that identity systems be resilient under varied connectivity conditions.

A third point of comparison concerns institutional and ecosystem readiness, particularly the capacity for cross-government coordination and secure interoperability. Estonia's X-tee provides decentralised but standardised data exchange infrastructure that links identity credentials with government registries and services. Singapore's Myinfo and APEX ecosystem similarly demonstrate the reliance of Singpass on interoperable, securely governed data flows. India's Aadhaar architecture integrates with welfare delivery, payments and private digital services through APIs such as e-KYC and Aadhaar-enabled Payment Services. The World Bank's ID4D Principles emphasise that digital identity must be treated as critical public infrastructure requiring open standards, transparent governance and comprehensive risk management throughout its lifecycle. Malaysia therefore cannot emulate only the visible elements of MyDigital ID such as SSO without simultaneously maturing broader institutional capabilities including registry governance, cybersecurity, incident response and inter-agency coordination. Without

these foundations, Malaysia faces the same systemic risks encountered in countries where identity systems expanded faster than their supporting governance structures. These differences help explain why digital identity systems encounter distinct risks during implementation, even when their overall design appears robust.

3.6. Implementation Challenges

The experiences of Estonia, Singapore and India highlight a set of implementation challenges and pitfalls that offer important lessons for countries developing or expanding digital identity systems.

Integrity of registration, credentials and data is a recurring implementation challenge across Estonia, Singapore and India. Estonia's experiences shows that even mature, highly trusted digital identity systems remain vulnerable. The country faced a major security risk related to the chips used in its eID cards in 2017 which required the revocation and replacement of affected cards[147]. The vulnerability was identified as an algorithmic flaw that theoretically allowed an attacker to calculate the private key from the public key, affecting approximately 800,000 eID cards issued since 2014. In 2024, a major security breach happened at an external service provider, Allium UPI, which manages loyalty card systems for Estonian retail brands, where attackers stole nearly 700,000 PICs[148]. Singapore's vulnerabilities emerge from user-targeted compromise. Public reporting in 2024 documented the circulation of Singpass credentials on illicit platforms, enabled largely by phishing, malware and poor endpoint security rather than system design flaws[149]. India presents another scenario, where widespread operator access and inconsistent security controls led to unauthorized entry into Aadhaar enrolment and authentication portals, enabling large amounts of personal data to be queried or exposed through misconfigured systems. In early 2018, the unrestricted access to the database could be purchased for a nominal fee as unauthorized agents sold login credentials that provided a gateway to personal details via an official portal[150]. The exposed data included personally identifiable information such as name, address, photograph, phone number and email address.

Governance, privacy and surveillance concerns arise in all three jurisdictions, reflecting how institutional arrangements shape public confidence and the responsible use of digital identity. Estonia utilises PIC as a unique identifier across domains, which generates concerns related to profiling and linkage. The PIC is designed to reveal specific attributes, including gender, century of birth and date of birth. Utilizing this unique identification number streamlines the connection of fragmented identity information across multiple databases. This concentration of data makes the enforcement of data privacy and access controls essential[151]. Singapore highlights the importance of stable and transparent purpose limitation, as illustrated by the TraceTogether[152]. The implementation of TraceTogether involved an initial assurance that the data collected would only be used for COVID-19 contact tracing purposes. However, public trust was eroded when the

[147] Estonian Business and Innovation Agency (2018)
[148] Information System Authority (RIA) (2025b)
[149] Diresta and Larkin (2025)
[150] Burgess (2025)
[151] World Bank (2014)
[152] Teo and Harjani (2021)

government made an "unexpected U-turn" after disclosing that existing Criminal Procedure Code provisions covered the use of this data for criminal investigations. India's journey highlights the risks of deploying a large-scale identification platform without an adequate pre-existing legal and oversight framework. India historically lacked a comprehensive privacy law to regulate the use of personal data by entities such as the UIDAI, banks, and telecom providers, sparking widespread debate over privacy and government surveillance due to the extensive collection of personal and biometric data, as well as the merging of various databases[153]. The Supreme Court's 2018 ruling recognized the system's usefulness for efficient subsidy delivery but also struck down several provisions aimed at protecting privacy and individual rights[154]. For example, the Court held that the compulsory linking of Aadhaar to bank accounts and mobile SIM cards was unconstitutional because it did not meet the proportionality test and lacked legislative backing. Additionally, the Court partially upheld the mandatory use of Aadhaar for government subsidies and benefits but ruled that Aadhaar could not be required for services that are constitutional entitlements, such as elementary education, or for services not specifically provided by the government.

Inclusivity, accessibility and the risk of exclusion continue to shape national identity outcomes, and the experiences of Estonia, Singapore and India illustrate the consequences of inadequate design attention to user diversity. Estonia's success in digital service uptake does not eliminate challenges encountered by older adults or individuals with limited digital literacy, who may struggle with multi-step authentication or hardware requirements[155]. Estonia has proactively engaged in efforts to address accessibility, including implementing activities aimed at assisting the population in using the digital tools, specifically focusing on reaching senior citizens. Singapore confronts similar issues, with official advisories noting a disproportionate impact of scams on older users[156], revealing that secure authentication alone does not guarantee equitable use when digital risks vary across age groups. India illustrates more severe exclusion risks, where authentication failures, gaps in enrolment records or poor connectivity contributed to documented cases of individuals being unable to access welfare schemes tied to Aadhaar verification[157].

Sustainability, vendor dependence and long-term resilience also shape the trajectory of digital identity systems, as shown in the operational experiences of Estonia, Singapore and India. Estonia's highly interconnected ecosystem has required continuous investment in infrastructure upgrades and cyber defence, particularly after vulnerabilities revealed the limitations of relying on a single chip manufacturer for secure credential production[158]. Singapore's transition from earlier, less flexible on-premises architectures to cloud-based platforms demonstrates that initial design choices can constrain scalability and operational responsiveness as service demands evolve[159]. India shows that while open standards and modular design reduce vendor lock-in,

[153] Burgess (2025)
[154] Supreme Court Observer (2018)
[155] World Bank (2014)
[156] Diresta and Larkin (2025)
[157] Supreme Court Observer (2018)
[158] Estonian Business and Innovation Agency (2021); (2018)
[159] World Bank (2022)

large-scale systems still require sustained financing, ongoing cybersecurity resources and governance arrangements capable of addressing distributed operational responsibilities[160].

Together, these cases show that weaknesses in security, governance, inclusion and system resilience can undermine trust and effectiveness as digital identity systems scale, the risks that Malaysia will need to anticipate as MyDigital ID expands beyond SSO. Malaysia's current SSO phase therefore resembles the initial stages observed across these three systems, positioned to mature through phased legal and institutional evolution.

[160] Banerjee (2016)

4. Malaysia's MyDigital ID

4.1. Determinant Analysis

MyDigital ID[161] is Malaysia's national digital identity and authentication platform, enabling secure verification, login and digital signing for government and regulated private services. Currently, MyDigital ID integrates with several government service applications, including MyBayar, MyGov, MyJPJ, MySTR and MyTax. The integration also extends to a few private company applications like CTOS, Kayaaku Wallet, MyEG and TNB.

Integrity of Registration and Credentialing is established through a registration and authentication model that verifies identity directly against authoritative government databases without storing personal or biometric data on the platform itself, positioning MyDigital ID as a secure online identification layer that complements rather than replaces MyKad for physical identification. Registration follows a defined eKYC workflow comprising email and OTP verification, entry of name and identity card number, MyKad image capture and live facial scan, after which a digital certificate is issued to the user's device; a pre-registration function further validates name and IC number in advance to streamline full onboarding, including via physical kiosks located at JPN branches, National Information Dissemination Centres and selected service outlets.

Credential lifecycle controls allow users to revoke and renew certificates, for example in cases of device loss, while local device biometrics such as fingerprint or facial recognition are supported for everyday authentication. Security is underpinned by internationally recognised encryption and authentication standards, certified digital certificates, secure message signing and compliance with Common Criteria EAL 3+[162], alongside digital signatures issued through licensed Certification Authorities under the Digital Signature Act 1997. The system is further reinforced by patented technologies developed by MIMOS covering secure authentication, access control, transaction signing and key management. MyDigital ID therefore exhibits design features that support the integrity, security and reliability of registration and credentialing, including validation against authoritative databases, enforced uniqueness through system rules and facial verification, cryptographic binding of credentials to the individual's identity, non-retention of biometric data, and a high-assurance authentication architecture designed to mitigate risks of data breaches and identity theft while enabling trusted SSO across government digital services.

[161] All information related to MyDigital ID is obtained from the MyDigital ID portal (https://www.digital-id.my/), unless stated otherwise.

[162] MIMOS Berhad (2023).

Notes: The Common Criteria (EAL 3+) certificate, an international standard for IT security evaluation, confirms that MyDigital ID has been independently tested and certified for secure digital authentication and signing in accordance with globally recognised cybersecurity assurance standards. Details are available at commoncriteriaportal.org and in the official certificate.

Functionality and Interoperability are currently centred on its role as an SSO credential for government and regulated digital services, with adoption accelerating during 2025. In the second quarter of 2025, registrations stood at 2.8 million users and have since risen to approximately 8.7 million, while integration has expanded to more than 80 applications[163]. In 2025, the government has signalled a major scale-up phase by setting a target of up to 15 million registered users and prioritising integration across key sectors such as finance, telecommunications, e-commerce and health[164]. Functionally, MyDigital ID enables streamlined access to services through a single set of credentials, supports QR-code-based portal login and transaction signing, and facilitates 24-hour access to digital services, reducing user friction and transaction time.

Interoperability is supported domestically through secure, real-time verification against authoritative government databases, without storing personal data on the platform, and is complemented by partnerships, such as those with CTOS Digital, to strengthen eKYC capabilities. Published technical standards, including X.509, ISO/IEC 9798-3 and RFC 7515, suggest alignment with widely used open cryptographic protocols that enable secure API-based integration, although the patent-based architecture reflects sovereign innovation and the openness of licensing arrangements for third-party integration remains unclear. This indicates that the system is primarily designed to enhance usability, streamline access to services, and support integration across government and regulated private sectors. The passage of the National Registration (Amendment) Act 2025 provides statutory recognition for MyDigital ID across both domains[165]. While the Act has been approved, its operational implications for private-sector reliance, enforcement mechanisms and cross-sector interoperability will depend on subsidiary regulations and implementation practice. Implementation to date has focused on platform onboarding, online authentication, and managed device portability through de-registration and re-registration processes. MyDigital ID remains complementary to MyKad and does not substitute for physical or in-person identity verification.

Governance, Oversight and Safeguards are organised within a coordinated, multi-agency framework that assigns specific responsibilities across policy, implementation and security functions. Strategic coordination is exercised through MED4IRN, chaired by the Prime Minister, and the IDN chaired by the Minister of Home Affairs, which together guide policy coherence and oversee implementation. MyDigital ID Sdn. Bhd. serves as the implementing entity, with the JPN providing authoritative identity verification, MIMOS Berhad is responsible for developing and maintaining the technical infrastructure. MIMOS Berhad played a key role in developing the system's technological foundation during the early stages. Governance responsibilities for MyDigital ID have evolved over time. Responsibility for managing and operating MyDigital ID has since been assigned to MyDigital ID Sdn. Bhd., while technical development and system support functions may also be delivered through external vendors engaged via government procurement processes. Cybersecurity assurance and incident response are led by the National Cyber Security Agency, while the National Security Council provides overarching national security coordination. These agencies are involved indirectly, as part of their standing mandates over national digital and security infrastructure, rather than through MyDigital ID-specific governance arrangements.

[163] Malay Mail (2025); BERNAMA (2026)
[164] BERNAMA (2025b)
[165] BERNAMA (2025a)

Communication-related matters fall under the Ministry of Communications, in line with its general responsibility for government communications.

The platform has been independently evaluated under the international certification scheme (Common Criteria EAL 3+) at a high assurance level and operates on a privacy-by-design basis by verifying identities directly against government databases without storing personal or biometric data. In parallel, MIMOS has operationalised the Malaysia Blockchain Infrastructure (MBI), developed with MyEG, illustrating how adjacent DPI layers including blockchain-based verifiable credentials[166] may increasingly intersect with MyDigital ID and underscoring the importance of clearly delineating governance roles, assurance objectives and accountability across platforms. From a legal perspective, the National Registration (Amendment) Act 2025 passed in August 2025, officially establishes statutory recognition of MyDigital ID within the national identification system. Public-sector data sharing is governed by the Data Sharing Act 2025, while private-sector processing remains regulated by the Personal Data Protection Act 2010.

Inclusivity and Accessibility are shaped by a deliberately multi-channel enrolment and access model that seeks to extend digital identification beyond fully online users, while remaining structurally dependent on foundational identity and basic digital access. Registration is available through online self-enrolment, physical kiosks and assisted pre-registration counters, with kiosks deployed at selected shopping malls, retail outlets and government offices nationwide to allow walk-in registration without prior appointments. These assisted channels function as an important bridge for users with lower digital confidence, while usability is further enhanced through QR-code login and local device-based biometric verification, which reduces friction for repeated authentication.

At the same time, eligibility is currently restricted to MyKad holders, excluding non-MyKad populations such as foreign residents. Online enrolment requires access to a smartphone and internet connectivity, even when physical kiosks are used. Inclusivity is implicitly reinforced through integration with social protection platforms such as the Rahmah cash aid portal, allowing beneficiaries of government assistance to access services digitally, while affordability is addressed indirectly through efficiency gains that reduce travel, waiting time and opportunity costs associated with physical counter services. However, publicly available information on adoption remains limited, with infrequent updates, no disaggregated data by location, gender or age, and no published national inclusion strategy addressing enrolment challenges among rural communities, senior citizens or persons with disabilities. As a result, while MyDigital ID includes assisted mechanisms and maintains MyKad for physical identification, accessibility results remain inconsistent and depend on existing documentation and digital resources rather than being guided by a comprehensive inclusion policy.

[166] MIMOS Berhad (2025)

Sustainability and System Design Models in MyDigital ID reflect an approach oriented toward long-term viability, resilience and vendor neutrality, anchored in sustained government commitment and a non-centralised data architecture. Positioned within the broader GovTech agenda, MyDigital ID benefits from continued political support and dedicated public funding for digitalisation initiatives, while its design enhances sustainability by relying on real-time reference to authoritative government databases rather than maintaining separate identity records. This approach preserves data integrity by aligning with civil registration systems and reducing operational duplication. System resilience is reinforced through compliance with internationally recognised standard, cryptography-based authentication and a unified SSO architecture that supports incremental integration of new services. Legal adaptability is further supported by amendments to the National Registration Act 1959, which extend the applicability of MyDigital ID across both public and private sectors. Vendor neutrality is achieved through strict data minimisation, the explicit exclusion of biometric and personal data storage, and operation as a validation and authentication layer rather than a data repository, enabling the system to remain technology-agnostic while interoperating with sectoral eKYC standards and trusted partners.

Overall, MyDigital ID's integrity is supported by MyKad-linked eKYC, biometric verification and credential lifecycle controls, including certificate renewal and revocation. Its functionality centres on secure authentication and digital signing across integrated services, including QR-based login, and is built on internationally recognised encryption and authentication standards. Governance arrangements outline clear operational and technical roles, while arrangements for independent oversight and user redress have yet to be fully detailed in publicly available materials. Inclusivity is addressed through multi-channel onboarding mechanisms, although publicly available data on adoption and a consolidated national inclusion strategy remain limited. Sustainability is reflected in integration with national digital platforms and a cryptography-based system design, with further clarity on funding models, vendor-neutrality arrangements and audit practices expected as the system matures.

Taken together, available information suggests that MyDigital ID is currently positioned as a secure and scalable SSO capability, supported by formal certification, standards alignment and expanding integration across government services. These features provide a foundation for its potential evolution into a broader digital identity ecosystem, alongside the continued development of legal oversight, interoperability governance, inclusion monitoring and long-term resourcing frameworks.

4.2. Comparative Positioning

Malaysia's MyDigital ID marks the country's first coordinated step toward a secure national digital identity ecosystem. At its present SSO phase, the platform performs functions once undertaken by Estonia, Singapore and India during their early identity-system development: verifying user credentials, providing unified log-in, and coordinating access across agencies. As those countries' experience shows, effectiveness at the SSO level depends not only on technology but also on legal authority, interoperability design, and citizen trust.

This comparison therefore proceeds in two stages as shown in Figure 5:

- Stage 1: Malaysia's present MyDigital ID compared with the early SSO performance of Estonia, Singapore and India; and
- Stage 2: Malaysia's trajectory toward foundational interoperability compared with the current mature systems of the same countries.

Figure 5: Comparative Positioning of MyDigital ID against e-ID, Singpass and Aadhaar

Analytical Determinants	Stage 1: SSO Stage	Stage 2: Transition to Maturity Stage
Integrity of Registration and Credentialing	All four systems achieve high identity assurance by verifying identity claims against pre-existing national authoritative sources established in law. Estonia relies on permanent civil registration under the Population Register Act, using the PIC as the sole identifier and excluding biometrics. Singapore anchor's identity in the NRIC or FIN under the National Registration Act 1965, complemented by biometric enrolment for deduplication and verification. India relies on large-scale multimodal biometric enrolment under the Aadhaar Act 2016, highlighting gaps in its civil registry. Across cases, credential security and recognition are statutory, with Estonia's model providing the strongest legal status through EU recognition of its digital certificates as a Qualified Signature Creation Device (QSCD). **Malaysia achieves high integrity and assurance by validating MyKad holders against authoritative databases through an administrative process, supported by mandatory live**	Estonia, Singapore and India emphasise continuous cryptographic assurance and mitigation of identity theft risk through both technical and legal measures. Estonia maintains high assurance through legally mandated digital certificates with QSCD status, continuous IT security monitoring in accordance with national standards, and a credential lifecycle recognised under EU law. Singapore maintains assurance through the ongoing refinement of biometric verification and public key infrastructure processes, which support credential renewal and account recovery. India reinforces integrity by introducing architectural safeguards, such as Virtual ID and tokenisation, to protect the unique identifier and prevent link ability, which are developed and enforced within its legislative framework. **Malaysia needs to formalise and publicly clarify long-term credential lifecycle processes, including renewal, device migration, and certificate revocation, to meet continuous assurance standards. Legal and institutional maturity now depends on the effective**

Analytical Determinants	Stage 1: SSO Stage	Stage 2: Transition to Maturity Stage
	facial scanning and system-based deduplication. The system design is compliant with international standards and digital certificates are legally recognised under the Digital Signature Act 1997, ensuring the validity of cryptographic credentials.	**implementation of the National Registration (Amendment) Act 2025 to secure ongoing statutory integrity.**
Functionality and Interoperability	Estonia, Singapore and India provide SSO functionality that enables reuse of digital identity across services, with differences arising in scale and enabling mechanisms. In Estonia and Singapore, digital ID and SSO functionality are underpinned by legislation that supports interoperability and electronic transactions, facilitating widespread adoption of online services. In India, SSO and API based integration are supported by authentication provisions under the Aadhaar Act. Across all cases, the digital identity is statutorily recognised and functions as a foundational credential for state and market interactions. **Malaysia currently functions as a SSO credential for government and regulated services, with SSO functionality relying on open cryptographic protocols at the technical and administrative level. Adoption remains low, which constrains the economic impact. Statutory recognition for broader private-sector adoption has been approved under the National Registration (Amendment) Act 2025. However, legal certainty for enforcement, reliance obligations and cross-sector scalability will depend on implementation and regulatory follow-through.**	Estonia achieved near-universal adoption, enabling efficiency gains and the creation of digital public goods, while Singapore embedded MyInfo across extensive public and private services, generating very high transactional volumes. Both Estonia and Singapore actively pursue cross-border interoperability through formal policy and legislative mandates. This scale is underpinned by statutory recognition of digital credentials, which enables mandatory integration across regulated sectors, such as finance and healthcare. India similarly achieved scale through a strong legal foundation that enabled deep, API-based integration across the economy. **Malaysia needs to meet its user targets to reach critical mass and system maturity. Functional maturity also requires the deployment of transaction signing and clear licensing or openness terms for its patent-based architecture, enabling private sector integration and innovation. Legal certainty is necessary to encourage private sector reliance and facilitate broader economic integration, while cross-border ambitions remain aspirational.**

Analytical Determinants	Stage 1: SSO Stage	Stage 2: Transition to Maturity Stage
Governance, Oversight and Safeguards	All systems emphasise privacy-by-design, with differences in governance and legal structure. Estonia provides the strongest model, constitutionally protecting privacy, mandating independent oversight, and granting citizens statutory rights to access tamper-proof audit logs of data use. India relies primarily on architectural safeguards, including non-shared core biometrics and a non-semantic unique identifier, with governance established through the Aadhaar Act 2016. Singapore employs a whole-of-government model that combines central coordination and consent-based data sharing, supported by legislation on registration and electronic transactions, with personal data protection primarily applicable to the private sector. In all three cases, the authority and legal standing of digital identity systems are rooted in primary legislation. **Malaysia operates under a coordinated multi-agency framework and applies a privacy-by-design approach through real-time identity verification, without storing personal or biometric data. Its legal basis currently relies on the Personal Data Protection Act 2010, Data Sharing Act 2025 and National Registration (Amendment) Act 2025. Mechanisms for independent oversight and transparent user access to audit trails are not publicly available, indicating the need for a clearer legal mandate and oversight framework.**	The focus across the three systems is user control, enforcement transparency, and certainty of independent oversight, implemented through differing legal and technical approaches. Estonia provides the strongest statutory model, mandating user access to tamper-proof audit logs and enforceable penalties under the Public Information Act, with accountability supported by judicial oversight. India relies primarily on architectural safeguards such as a unique identifier and Virtual ID, complemented by Supreme Court rulings that defined limits on data retention and strengthened accountability. Singapore emphasises administrative and regulatory controls through advanced fraud analytics and strict consent management mechanisms embedded in MyInfo. **Malaysia's governance should enhance inter-agency coordination to promote transparency and establish independent enforcement by passing and effectively implementing the amended National Registration Act 1959 and the Data Sharing Act 2025. This transition requires establishing an independent oversight body, providing public access to audit reports and enacting a right for users to access audit logs of data usage. These measures are crucial for ensuring accountability and building public trust, bringing governance maturity in line with comparable systems.**

Analytical Determinants	Stage 1: SSO Stage	Stage 2: Transition to Maturity Stage
Inclusivity and Accessibility	All systems aim for universal coverage and rely on multimodal access points, while differing in how inclusion is ensured through law and policy. Estonia mandates universal coverage through the Population Register Act, embedding inclusion from birth registration for all residents. India's framework, established under the Aadhaar Act 2016, includes a specific legislative safeguard requiring the provision of alternate and viable means of identification when digital or biometric authentication fails, addressing risks of exclusion. Singapore's approach is grounded in the National Registration Act 1965 covering citizens and legal residents, complemented by administrative and policy measures that emphasise user experience testing, multilingual support across the four official languages, and the maintenance of physical service centres. **Malaysia offers multi-channel access through online enrolment, kiosks and assisted counters, but eligibility remains restricted to MyKad holders, excluding legal non-MyKad residents. The absence of a published national inclusion strategy and disaggregated adoption metrics indicates a monitoring gap, underscoring the need to expand eligibility and formalise a data-driven inclusion approach.**	Estonia, Singapore and India are actively mitigating digital exclusion and ensuring access for underserved groups through statutory and administrative measures. India maintains a legislative mandate requiring alternate means of identification when digital methods fail, preserving access for vulnerable populations. Estonia and Singapore sustain universal coverage through foundational identity laws, while Singapore further supports inclusion through continued investment in accessibility, multilingual design and assisted physical service centres. Across these systems, monitoring and evaluation practices collect and use adoption and usage data to inform policy adjustments and address inclusion gaps. **Malaysia needs to determine and implement a clear policy to expand legal eligibility beyond MyKad holders to all legal residents. This requires a formal, publicly defined inclusion strategy supported by transparent and disaggregated monitoring and evaluation data, with clear policy mandates to target rural and low digital literacy populations and ensure equitable access.**

Analytical Determinants	Stage 1: SSO Stage	Stage 2: Transition to Maturity Stage
Sustainability and System Design Models	Estonia, Singapore and India prioritise long-term viability through digital, foundational design, open standards, modularity, and vendor neutrality. Estonia ensures resilience through a decentralised, open-source architecture supported by national security standards. India promotes sustainability and cost efficiency through a legislated "Identity in the Cloud" architecture. Singapore relies on foundational data and a centralised whole-of-government gateway to enforce common data standards as an administrative structure **Malaysia utilises a non-centralised data architecture that verifies identity against authoritative databases without storing personal data aligned with cost-efficient and secure sustainable system design. Technical resilience is validated through Common Criteria EAL 3+ certification, while the use of open cryptographic protocols supports vendor neutrality.**	The focus across the three systems is financial sustainability, infrastructure scalability, and continued technological neutrality. Estonia and India demonstrate cost-efficient architectures that support long-term sustainability through low operational expenditure, while Singapore sustains scalability and resilience through continuous investment in core government technology infrastructure. Open standards and modular design are prioritised to maintain vendor neutrality, with Estonia reinforcing this through continued open-source development and India anchoring its cost-saving model within a legislative framework. **Malaysia's system architecture demonstrates resilience, but greater transparency is required on the long-term financial model and funding sources for operations and maintenance. A clear financial sustainability plan and specified audit schedules are necessary to provide confidence in the system's longevity and ensure that ongoing operations are not vulnerable to political or fiscal fluctuations.**

Source: Author's table, synthesised from digital identity frameworks by the World Bank, UN, OECD and WEF, alongside policy documents, official websites, and reputable sources relating to MyDigital ID, e-ID, Singpass and Aadhaar

Malaysia has developed a solid technical design for high assurance and has achieved initial SSO capability, supported by high credentialing standards and a resilient, decentralised data architecture. Progress at the SSO and maturity stages however has been more measured due to the absence of statutory recognition and evolving governance arrangements. This contrasts with the strong legislative mandates that have enabled widespread adoption and high transaction volumes in Estonia, Singapore and India. As long-term assurance processes are formalised, legislative certainty is established, and independent and transparent oversight is implemented, Malaysia's digital identity system is expected to advance toward greater operational and institutional maturity.

5. Optimising Implementation

Malaysia's MyDigital ID is transitioning from an early-stage authentication platform toward a more integrated digital identity infrastructure. The institutional foundations have been established to provide a strong administrative framework. The next phase is to strengthen the system's operational integrity, institutional coordination and legal coherence while deepening inclusivity, resilience and innovation. The following policy recommendations focus on practical actions and strategic directions that consolidate these goals.

5.1. Strengthening Legal and Regulatory Frameworks

Legal coherence is crucial in establishing MyDigital ID as a rights-based component of Malaysia's digital public infrastructure. While MyDigital ID currently operates within existing administrative and sectoral legal frameworks, there is no single statute that comprehensively governs the full operational lifecycle of public sector digital identity authentication, credential use and associated rights and obligations. Existing laws provide partial coverage, most notably through the Personal Data Protection Act 2010 for private sector data processing and the Data Sharing Act 2025 for inter-agency data exchange. These laws do not fully address the legal status, accountability and user protections associated with a national digital identity credential.

Recent amendments to the National Registration Act 1959 strengthen the security of foundational identity records and formally recognise MyDigital ID as part of the national digitalisation agenda, while preserving the primacy of the physical identity card. However, these amendments do not yet provide a comprehensive legal framework governing digital identity credentials, authentication use, or associated user rights and obligations.

At this stage of implementation, legal certainty can be strengthened through clearer operational practices within existing laws. Formalising standard operating procedures for consent management, credential revocation, incident handling and grievance redress would reduce ambiguity and support consistent implementation across agencies. Strengthened transparency and accountability practices can further reinforce public confidence while broader legal consolidation is pursued.

As MyDigital ID becomes more deeply embedded across public services and regulated sectors, a dedicated statutory framework becomes increasingly important to ensure continuity, legitimacy and alignment with international practice. Such a framework should anchor MyDigital ID as a recognised national digital identity credential while preserving operational flexibility and avoiding regulatory duplication.

Policy Considerations

To provide legal certainty and enforceability, the governance of MyDigital ID should be anchored in a statutory framework that clearly defines its status, scope and safeguards. The legal framework should establish the status and function of MyDigital ID credentials, including their recognition for authentication and digital signing, to ensure clarity for public sector use and regulated private sector reliance. It should secure user rights, including rights to informed consent, correction of inaccurate information, credential revocation and access to grievance redress. This embeds digital identity within a rights-based governance framework.

Clear provisions should further define accountability and liability, including consequences for misuse, negligence or unauthorised access. This supports trust and deters abuse across the digital identity ecosystem. Transparency obligations should include regular public reporting on privacy protection, security incidents and system performance. These measures reinforce public confidence and institutional accountability.

Operational clarity should be supported through articulated procedures for consent management, credential lifecycle control, incident response and grievance handling. These measures enable consistent implementation without constraining technical adaptability. Independent cybersecurity audits, coordinated by the National Cyber Security Agency and accompanied by public disclosure of non-sensitive findings, should complement these safeguards and strengthen oversight in practice.

Alignment with existing obligations under the Personal Data Protection Act 2010 and the Data Sharing Act 2025 should be achieved through cross-referenced provisions. This avoids regulatory overlap while ensuring comprehensive coverage. Reliance on licensed certification authorities under the Digital Signature Act 1997 should be maintained. This preserves legal continuity and separates operational identity management from the responsibilities of the certification authority.

5.2. Enhancing Institutional Governance

Malaysia's digital identity initiative operates within an established governance structure supported by national level coordination mechanisms and a defined institutional ecosystem. As MyDigital ID expands in scope and usage, governance effectiveness increasingly depends on clarity of mandates, coordination across institutions and consistent accountability.

Several public sector functions are essential to the governance of MyDigital ID. Strategic oversight is exercised through national level coordination mechanisms. Policy leadership sits within the Ministry responsible for digital development. Operational responsibility for implementation currently rests with MyDigital ID Sdn. Bhd. Authoritative identity verification is provided by the National Registration Department. Cybersecurity assurance and security oversight are undertaken by the National Cyber Security Agency. Technical development and system operation are functions that may be delivered by designated entities in accordance with government administrative arrangements.

As reliance on MyDigital ID increases across public services and regulated sectors, governance effectiveness depends less on the permanence of specific entities and more on the clarity of functional responsibilities and reporting relationships. Institutional arrangements should therefore be designed to remain stable even if delivery structures or corporate forms change over time. The implementation history of MyDigital ID illustrates this dynamic in practice. Responsibility for system development, management and operation has evolved over time, reflecting changes in institutional arrangements and delivery models. While such evolution is a normal feature of public digital infrastructure, it reinforces the importance of governance arrangements that preserve continuity of purpose, safeguards and accountability regardless of which entities are responsible at any given point.

Policy Considerations

Governance arrangements for MyDigital ID should be clarified and reinforced through explicit allocation of functional responsibilities within existing institutional structures. As MyDigital ID expands in scope and operates alongside other DPI components, strategic oversight of digital identity policy should continue to be exercised through national-level coordination mechanisms, with responsibility for setting direction and resolving cross-sector issues. Policy leadership should remain with the Ministry responsible for digital development, including responsibility for standards setting, sectoral integration and overall system performance.

Operational implementation should be assigned to the designated delivery entity responsible for MyDigital ID, with clear accountability for coordination, system management and service delivery. Authoritative identity verification should remain with the National Registration Department. Cybersecurity assurance and security oversight should remain with the National Cyber Security Agency, particularly as identity services become more interconnected with wider digital platforms and trust infrastructures.

Technical development and system operation should be governed through clearly defined functional mandates and contractual or administrative arrangements, rather than reliance on any single institution. This approach ensures continuity of governance and accountability, even as delivery structures evolve or adjacent DPI layers emerge, thereby reducing the risk of mandate overlap or fragmentation.

Reporting on adoption, system integration and security status should be consolidated across responsible entities to support informed strategic oversight and timely policy adjustment. Governance reform should prioritise mandate clarity, reporting consistency and accountability. The creation of additional councils or parallel coordinating bodies is not required and may weaken responsibility rather than strengthen it.

5.3. Building Public Trust

Public trust plays a role in both the initial uptake and the long-term sustainability of digital identity systems. In early stages, adoption is influenced by a combination of factors including service availability, ease of use and perceived value, alongside confidence in how identity credentials are managed. As MyDigital ID becomes more widely integrated across public and private services, trust becomes increasingly important because users are asked to rely on the system more frequently and in more consequential contexts.

At this stage, trust can be reinforced through measures that make safeguards and accountability visible to users and the public. Public communication has focused on explaining key system features, including the process of identity verification. As reliance on MyDigital ID increases, confidence will depend increasingly on what users can observe in practice, such as system reliability, security assurance and clear accountability arrangements.

Trust is also shaped by how effectively user concerns are handled. Support and help desk channels are already available to assist users. Their effectiveness depends on visibility, responsiveness and clarity about how issues are addressed. Making these processes more

structured and transparent can strengthen confidence and ensure that user feedback contributes to ongoing system improvement.

Over time, trust should be reinforced through predictable and consistent accountability arrangements. Transparency, reporting and redress should be built into digital identity governance as part of its normal operation. This helps ensure that confidence in MyDigital ID is maintained as integration and reliance deepen.

Policy Considerations

Public trust in MyDigital ID should be strengthened through transparency, accountability and user protection measures that evolve alongside system expansion.

Transparency should be delivered through publicly accessible channels that present consolidated information on system availability, adoption progress and security assurance in a clear and understandable manner. These channels should allow the public to observe system reliability and oversight without requiring technical knowledge.

User support, grievance and redress should be strengthened by formalising existing channels into a clearly defined process. This includes making support entry points visible, setting expectations for response times and providing users with confirmation and follow up when issues are raised. Feedback from these processes should be reviewed systematically to inform service improvements and risk management.

Accountability should be reinforced through regular public reporting on system performance, security incidents and complaint handling. Independent audits and reviews should complement these disclosures to ensure credibility. Findings from reporting and audits should inform governance oversight and policy adjustment.

5.4. Promoting Inclusion and Accessibility

Inclusive access is essential to ensuring that digital identity functions as public infrastructure rather than a barrier to participation. Digital identity systems that scale without deliberate attention to inclusion risk reinforcing existing inequalities related to digital inclusion and literacy. As MyDigital ID expands in use and integration, inclusion and accessibility must therefore be treated as core implementation concerns that need to be actively assessed.

MyDigital ID has established multiple assisted enrolment channels. Registration kiosks are available in major shopping malls, selected retail outlets and government offices. In addition, MyDigital ID kiosks are located within community-based facilities that provide internet access and assisted digital services, particularly in rural areas and locations with limited internet connectivity. These arrangements create the conditions for inclusive access.

However, publicly available information on MyDigital ID adoption remains limited to aggregate enrolment figures. There is currently no published data on enrolment patterns by age group, location, disability status or use of assisted enrolment channels. As a result, it is not possible to assess with confidence whether older persons, rural communities or users with limited digital literacy are enrolling and using MyDigital ID at comparable rates.

In this context, inclusion challenges relate not only to the availability of access points, but also to visibility of participation outcomes and the ability to identify and address gaps. Ensuring inclusion therefore requires both optimisation of existing enrolment channels and improved understanding of who is being reached and who is not.

Policy Considerations

Inclusion and accessibility should be advanced through optimisation of existing enrolment infrastructure, inclusive system design and improved monitoring of participation outcomes.

Existing assisted enrolment channels, including kiosks in community-based facilities, government offices, and other public locations, should be supported through consistent operating standards, clear user guidance, and adequate on-site assistance. Outreach-based or mobile registration should be used selectively to complement existing facilities in areas where connectivity or access constraints persist.

MyDigital ID interfaces and relying services should adhere to recognised accessibility standards. This includes multilingual support and features that assist users with visual, hearing or cognitive impairments. Accessibility requirements should apply consistently across public sector services that integrate MyDigital ID.

To support evidence-based inclusion policies, enrolment and usage data should be analysed and reported in a manner that allows participation patterns to be understood. This includes distinguishing between assisted and self-service enrolment and presenting anonymised and aggregated indicators related to geographic coverage and levels of digital literacy.

Treating inclusion as an ongoing policy concern rather than a one-time rollout objective will enable adjustments to the implementation as MyDigital ID expands. Improved visibility of inclusion outcomes will help ensure that digital identity strengthens participation rather than reproduces existing digital divides.

5.5. Ensuring Technical Resilience

Technical resilience underpins confidence in digital identity systems and their ability to function reliably as public infrastructure. For MyDigital ID, resilience is not limited to cybersecurity strength, but also includes system continuity, secure interoperability and the capacity to respond effectively to operational stress as usage expands. As MyDigital ID supports a wider range of services, technical resilience must be maintained as an ongoing policy concern rather than treated as a one time technical achievement.

MyDigital ID has been designed with security and reliability as core requirements. As reliance increases across public services and regulated sectors, demands on system availability, incident response and recovery capabilities will intensify. Maintaining resilience therefore depends on the consistent renewal of safeguards and the alignment of operational practices with evolving risks and usage patterns.

Resilience should be understood as the system's ability to operate securely and predictably under routine conditions as well as during disruption. This includes preparedness for cybersecurity

incidents, system failures and integration related risks, alongside the capacity to adapt to changing technical and threat environments.

Policy Considerations

Technical resilience should be reinforced through sustained assurance practices, disciplined integration standards and planned operational resourcing.

Security assurance should be maintained through regular and independent assessment cycles that are renewed over time. These assessments should verify the continued effectiveness of security controls, incident response arrangements and recovery readiness as the system evolves.

System continuity should be supported through clearly defined redundancy and recovery arrangements. This includes maintaining backup capabilities, tested restoration procedures and operational protocols that minimise service disruption for users and relying services.

Interoperability should be governed through secure and consistent technical standards that reduce fragmentation and integration risk. Standards based integration supports reliability and security by ensuring that connections between systems remain predictable and manageable as MyDigital ID is adopted more widely.

Resilience requires planned and sustained resourcing. Ongoing budget allocation should support assurance activities, system upgrades and capacity management. Treating resilience as a continuous operational responsibility rather than a project milestone will help ensure that MyDigital ID remains reliable as reliance on the system grows.

Malaysia has established the core foundations of a national digital identity system, supported by institutional arrangements, operational capability and an expanding scope of use across public services. At the same time, MyDigital ID remains in a period of transition, evolving from an authentication platform toward a more integrated form of digital public infrastructure.

The policy directions set out above respond to this transition by focusing on consolidation rather than redesign. Legal and regulatory measures emphasise coherence, continuity and protection of user rights as digital identity use extends across sectors. Governance measures prioritise mandate clarity, coordination and stability to ensure consistent direction through administrative change. Trust and accountability measures recognise that confidence must be reinforced through visible safeguards and predictable processes as reliance deepens. Inclusion and accessibility measures build on existing enrolment infrastructure while addressing the need for clearer visibility of participation outcomes. Technical resilience measures treat security, reliability and continuity as ongoing responsibilities rather than one time achievements.

Taken together, these directions reflect a central insight. The priority is not to create new structures, but to strengthen alignment between law, institutions and operations so that MyDigital ID can scale securely and inclusively. Optimising implementation in this way provides a practical pathway toward a digital identity system that is reliable, trusted and capable of supporting Malaysia's broader digital transformation objectives.

6. Conclusion

MyDigital ID serves as an initial step in Malaysia's broader efforts to strengthen digital governance. Introduced as a national SSO authentication platform, it reflects a growing emphasis on secure and standardised access to digital services. At this stage, its significance lies not only in its technical function but also in the institutional and policy questions that accompany its development and use.

The analysis in this paper suggests that national digital identity initiatives are influenced by factors beyond technical design alone. Comparative experience suggests that such systems evolve within specific legal, institutional and social contexts, and that their effectiveness is closely linked to how these elements interact over time. In this sense, digital identity functions as a form of public infrastructure that requires ongoing coordination, oversight and public engagement, rather than a one-time technological solution.

In Malaysia's case, MyDigital ID incorporates design features intended to support security and data protection, while operating within a complex institutional environment involving multiple agencies and policy mandates. As observed in other countries examined in this paper, questions related to legal clarity, governance arrangements, inclusion and long-term stewardship often emerge progressively as systems expand and patterns of use become clearer. These issues are not unique to Malaysia, nor are they typically resolved at the point of system introduction.

International experience also suggests that public confidence in digital identity systems is influenced not only by system performance, but by how institutions communicate their purpose, manage risks and respond to concerns. Trust, in this context, appears to develop incrementally and can be shaped by broader perceptions of accountability and transparency. This reinforces the importance of viewing digital identity as part of a wider governance environment rather than as a standalone digital service.

In this context, MyDigital ID provides a useful case for examining how digital initiatives interact with existing administrative structures and public expectations. Its development offers an opportunity to reflect on how questions of access, safeguards and institutional responsibility are approached within Malaysia's digital transformation agenda. Experience from other jurisdictions suggests that such reflection often accompanies gradual adjustment and institutional learning, rather than following a fixed or predetermined path.

This discussion paper does not seek to prescribe a particular pathway for MyDigital ID. Instead, it aims to contribute to ongoing policy reflection by situating the initiative within international experience and highlighting considerations that may become relevant as the system continues to develop. How these considerations are addressed over time will shape the role of digital identity within Malaysia's broader approach to digital governance and public service delivery.

7. References

Banerjee, Shweta. 2016. 'Aadhaar: Digital Inclusion and Public Services in India'. *World Development Report*, 16.

BERNAMA. 2025a. 'Dewan Rakyat: Pindaan Akta Pendaftaran Negara selari pelaksanaan MyDigital ID'. Astro Awani. 26 August 2025. https://www.astroawani.com/berita-malaysia/dewan-rakyat-pindaan-akta-pendaftaran-negara-selari-pelaksanaan-mydigital-id-535905.

———. 2025b. 'Budget 2026: STAR Gets RM25 Mln To Drive Digitalisation, Innovation – PM Anwar'. BERNAMA. 10 October 2025. https://www.bernama.com/en/general/news.php?id=2477369.

———. 2026. 'MyDigital ID Targets 15 Mln New Registrations This Year'. BERNAMA. 17 January 2026. https://bernama.com/en/news.php/politics/business/news.php?id=2513621.

Burgess, Monica. 2025. 'Aadhaar Data Breach: What Happened, Impact, and Lessons | Huntress'. Huntress. 31 October 2025. https://www.huntress.com/threat-library/data-breach/aadhaar-data-breach.

Clark, Julia Michal, and Conrad Charles Daly. 2019. 'Digital ID and the Data Protection Challenge : Practitioner's Note'. Working Paper 142702. World Bank Group. https://documents1.worldbank.org/curated/en/508291571358375350/pdf/Digital-ID-and-the-Data-Protection-Challenge-Practitioners-Note.pdf.

Cyber Security Agency of Singapore. 2021. 'The Singapore Cybersecurity Strategy 2021'. ISBN: 978-981-18-2258-2. Cyber Security Agency of Singapore. https://ccdcoe.org/uploads/2018/10/Singapore_Cybersecurity_Strategy_2021.pdf.

Dahan, Mariana, and Randeep Sudan. 2015. 'Digital IDs For Development : Access To Identity And Services For All'. Brief 96254. World Bank Group. https://documents1.worldbank.org/curated/en/779711468000253531/pdf/96254-BRI-Box391421B-OUO-9-Transport-ICT-Newsletter-Note-13-v2.pdf.

Diresta, Renee, and CJ Larkin. 2025. 'Lessons from National Digital ID Systems for Privacy, Security, and Trust in the AI Age | TechPolicy.Press'. Tech Policy Press. 25 June 2025. https://techpolicy.press/lessons-from-national-digital-id-systems-for-privacy-security-and-trust-in-the-ai-age.

Economy Planning Unit of Malaysia. 2020. 'RMK12 - Twelfth Malaysia Plan, 2021-2025; A Prosperous, Inclusive, Sustainable Malaysia'. Ministry of Economy. 2020. https://rmke12.ekonomi.gov.my/en.

———. 2021. 'Malaysia Digital Economy Blueprint'. Economy Planning Unit, Prime Minister Department. https://ekonomi.gov.my/sites/default/files/2021-02/malaysia-digital-economy-blueprint.pdf.

Estonian Business and Innovation Agency. 2018. 'What we learned from the eID card security risk?' e-Estonia. 14 May 2018. https://e-estonia.com/card-security-risk/.

———. 2021. 'Estonian E-State Has Experienced Several Hacking Incidents as of Late: What Are the Lessons Learned? - E-Estonia'. E-Estonia. 18 August 2021. https://e-

estonia.com/estonian-e-state-has-experienced-several-hacking-incidents-as-of-late-what-are-the-lessons-learned/.

———. 2024. 'X-Road Interoperability Services'. Government. E-Estonia. Tallinn: e-Estonia. 2024. https://e-estonia.com/solutions/interoperability-services/x-road/.

———. 2025a. 'E-Identity'. Government. E-Estonia. 2025. https://e-estonia.com/solutions/estonian-e-identity/id-card/.

———. 2025b. 'Mobile ID - e-Estonia'. Government. E-Estonia. 2025. https://e-estonia.com/solutions/estonian-e-identity/mobile-id/.

———. 2025c. 'Smart ID - e-Estonia'. Government. E-Estonia. 2025. https://e-estonia.com/solutions/estonian-e-identity/smart-id/.

Information System Authority. 2025. 'Eesti App Will Get Proof of Identity Feature on 7 July | RIA'. Republic of Estonia Information System Authority. 2025. https://www.ria.ee/en/news/eesti-app-will-get-proof-identity-feature-7-july.

Information System Authority (RIA). 2024a. 'Situation in Cyberspace – March 2024'. Monthly situation report. Tallinn: Information System Authority (RIA). https://www.ria.ee/sites/default/files/documents/2024-04/Situation-in-cyberspace-march-2024.pdf.

———. 2024b. 'Situation in Cyberspace – September 2024'. Monthly situation report. Tallinn: Information System Authority (RIA). https://www.ria.ee/sites/default/files/documents/2024-10/Situation-in-cyberspace-september2024.pdf.

———. 2025a. 'Cyber Security in Estonia 2025'. Annual report. Tallinn: Information System Authority (RIA). https://ria.ee/sites/default/files/documents/2025-02/Cyber-security-in-Estonia-2025.pdf.

———. 2025b. 'Cyber Security in Estonia 2025'. Information System Authority (RIA). https://ria.ee/sites/default/files/documents/2025-02/Cyber-security-in-Estonia-2025.pdf.

———. 2025c. 'Eesti App Will Soon Be Available for Identity Verification'. Tallinn: Information System Authority (RIA). 9 June 2025. https://www.ria.ee/en/news/eesti-app-will-soon-be-available-identity-verification.

Malay Mail. 2025. 'With Only 2.8 Million Malaysians Registered, Putrajaya Mulls Law to Mandate MyDigital ID as Adoption Stalls'. *Malay Mail*, 21 July 2025, sec. Malaysia. https://www.malaymail.com/news/malaysia/2025/07/21/with-only-28-million-malaysians-registered-putrajaya-mulls-law-to-mandate-mydigital-id-as-adoption-stalls/184658.

MIMOS Berhad. 2023. 'MyDigital ID Streamlined Access and Enhanced Security'. 12 December 2023. https://www.mimos.my/implementation-of-mydigital-id/.

———. 2025. 'MIMOS Launches Malaysia Blockchain Infrastructure (MBI) to Drive Digital Economy'. Government. 17 June 2025. https://www.mimos.my/mimos-launches-malaysia-blockchain-infrastructure-mbi-to-drive-digital-economy/.

———. 2026. ‘A Digital Nation’s Journey: The MyDigital ID Memoir – From Sovereign Dream to Living Reality’. 2026. https://www.mimos.my/mydigitalid-digital-nation-journey/.

My Digital ID Sdn Bhd. 2025. ‘MyDigital ID’. 2025. https://www.digital-id.my/.

MyDigital ID Sdn Bhd. 2025. ‘MyDigital ID - FAQ’. MyDigital ID. 2025. https://www.digital-id.my/en/support#faq_support.

National Digital Department. 2019. ‘National Digital Identity Initiative’. Government. MyGovernment. 2019. https://www.malaysia.gov.my/portal/content/30592.

NEXT IAS. 2025. ‘UIDAI Notifies New Rules for Aadhar Authentication’. Next Generation Institute for UPSC Civil Services Examination Preparation. NEXT IAS. 2025. https://www.nextias.com/ca/current-affairs/01-02-2025/uidai-aadhar-authentication-new-rules.

Nordic Institute for Interoperability Solutions. 2025. ‘X-Road® Technology Overview’. X-Road. 2025. https://x-road.global/x-road-technology-overview.

Nortal. 2025. ‘Why Digital Sovereignty Matters and How X-Road Makes It Happen’. Nortal. 3 July 2025. https://nortal.com/insights/why-digital-sovereignty-matters-and-how-x-road-makes-it-happen.

OECD. 2011. ‘Digital Identity Management for Natural Persons: Enabling Innovation and Trust in the Internet Economy - Guidance for Government Policy Makers’. OECD Digital Economy Papers 186. Paris: OECD. https://www.oecd.org/content/dam/oecd/en/publications/reports/2011/11/digital-identity-management-for-natural-persons_g17a2066/5kg1zqsm3pns-en.pdf.

———. 2021. ‘G20 Collection of Digital Identity Practices’. OECD report. Paris: OECD. https://www.oecd.org/content/dam/oecd/en/publications/reports/2021/08/g20-collection-of-digital-identity-practices_51e4a5b9/75223806-en.pdf.

———. 2023. ‘Recommendation of the Council on the Governance of Digital Identity’. OECD. https://legalinstruments.oecd.org/en/instruments/OECD-LEGAL-0491.

———. 2024a. ‘Digital Public Infrastructure for Digital Governments, OECD Public Governance Policy Papers’. 68.

———. 2024b. *G7 Mapping Exercise of Digital Identity Approaches*. OECD Publishing. https://doi.org/10.1787/56fd4e94-en.

———. 2024c. ‘Digital Public Infrastructure for Digital Governments’. OECD Public Governance Policy Papers. 68th ed. OECD Public Governance Policy Papers. https://doi.org/10.1787/ff525dc8-en.

Personal Data Protection Commission (PDPC). 2022. ‘Advisory Guidelines on Key Concepts in the Personal Data Protection Act’. Advisory Guidelines. Singapore: Personal Data Protection Commission, Singapore. https://www.pdpc.gov.sg/-/media/files/pdpc/pdf-files/advisory-guidelines/ag-on-key-concepts/advisory-guidelines-on-key-concepts-in-the-pdpa-17-may-2022.pdf.

PwC. 2020. ‘National Digital Identity (ID) Framework for Malaysia Public Consultation Report’. MCMC. https://www.mcmc.gov.my/skmmgovmy/media/General/pdf/Public-Consultation-Report_National_DI.pdf.

Republic of India. 2016. *The Aadhaar (Targeted Delivery Of Financial And Other Subsidies, Benefits And Services) Act, 2016*. https://uidai.gov.in/images/Aadhaar_Act_2016_as_amended.pdf.

Singpass. 2025. 'Singpass Developer Portal'. Government. Singpass {dev}. 2025. https://developer.singpass.gov.sg/.

Smart Nation Singapore. 2024. 'Smart Nation 2.0 A Thriving Digital Future for All'. Ministry of Digital Development and Information. https://file.go.gov.sg/smartnation2-report.pdf.

Supreme Court Observer. 2018. 'Constitutionality of Aadhaar Act: Judgment Summary'. *SCO Supreme Court Observer* (blog). 26 September 2018. https://www.scobserver.in/reports/constitutionality-of-aadhaar-justice-k-s-puttaswamy-union-of-india-judgment-in-plain-english/.

Teo, Yi-Ling, and Manoj Harjani. 2021. 'Smart Nation: Privacy Protection and Public Trust'. S. Rajaratnam School of International Studies. 2 February 2021. https://rsis.edu.sg/rsis-publication/rsis/smart-nation-privacy-protection-and-public-trust/.

UCL IIPP. 2025. 'Global State of DPI'. Excel. Institute for Innovation and Public Purpose, UCL. https://docs.google.com/spreadsheets/d/168wnnvAk7N_FxAlVUR9HGwKUxMQWx53rLeaWhS90R8Y/edit?pli=1&gid=1834066771#gid=1834066771.

UNCDF. 2022. 'The Role Of Electronic Transactions And National Digital Id Systems In The Digital Economy'. UNCDF / Policy Accelerator (United Nations Capital Development Fund). https://static1.squarespace.com/static/5f2d7a54b7f75718fa4d2eef/t/621d4545d668f30b5c35eab3/1646085472035/EN-UNCDF-Brief-ElectronicID-2022.pdf.

UNDP. 2023a. 'Accelerating the SDGs through Digital Public Infrastructure'. UNDP (United Nations Development Programme). https://www.undp.org/sites/g/files/zskgke326/files/2023-08/undp-g20-accelerating-the_sdgs-through-digital-public-infrastructure.pdf.

———. 2023b. 'UNDP Model Governance Framework for Digital Legal Identity System'. 2023. https://www.governance4id.org/.

———. 2023c. 'The Human and Economic Impact of Digital Public Infrastructure'. Case Study. New York: UNDP (United Nations Development Programme). https://www.undp.org/publications/human-and-economic-impact-digital-public-infrastructure.

———. 2024. 'From Access to Empowerment: Digital Inclusion in a Dynamic World'. UNDP Policy Centre / United Nations Development Programme. https://www.undp.org/sites/g/files/zskgke326/files/2024-05/undp_digital_inclusion_in_a_dynamic_world.pdf.

Unique Identification Authority of India (UIDAI). 2025a. 'Aadhaar Face Authentication Transaction Clocks 100 Crore Mark in FY 2024–25'. New Delhi: UIDAI. 2 April 2025. https://uidai.gov.in//images/FaceAuthTransation.pdf.

———. 2025b. 'Face Authentication Hits Record 15.87 Crore in June; 229.33 Crore Authentications in June 2025'. Press Release. New Delhi: UIDAI. https://uidai.gov.in/images/Press_Release-13.pdf.

United Nations. 2022. 'UNCITRAL Model Law on the Use and Cross-Border Recognition of Identity Management and Trust Services (2022) | United Nations Commission On International Trade Law'. 2022. https://uncitral.un.org/en/mlit.

WEF. 2016. 'A Blueprint for Digital Identity: The Role of Financial Institutions in Building Digital Identity'. Geneva: World Economic Forum. https://www3.weforum.org/docs/WEF_A_Blueprint_for_Digital_Identity.pdf.

———. 2018. 'Identity In A Digital World: A New Chapter In The Social Contract'. World Economic Forum. https://www3.weforum.org/docs/WEF_INSIGHT_REPORT_Digital%20Identity.pdf.

———. 2019. 'Reimagining Digital Identity: A Strategic Imperative'. World Economic Forum. https://www3.weforum.org/docs/WEF_Digital_Identity_Strategic_Imperative.pdf.

———. 2021. 'Digital Identity Ecosystems: Unlocking New Value'. https://www3.weforum.org/docs/WEF_Guide_Digital_Identity_Ecosystems_2021.pdf.

———. 2023. 'Reimagining Digital ID'. Insight Report. https://www3.weforum.org/docs/WEF_Reimagining_Digital_ID_2023.pdf.

World Bank. 2014. 'Digital Identity Toolkit - A Guide for Stakeholders in Africa'. World Bank Group. https://www.id4africa.com/articles/DigitalIDToolkitforAfrica2014EN.pdf.

———. 2015. 'Estonia: A Successfully Integrated Population-Registration and Identity Management System'. Country case study. Washington, DC: World Bank. https://documents1.worldbank.org/curated/en/873061495178335850/pdf/115147-WP-EstoniaIDPopregistryIDcasestudyNovweb-PUBLIC.pdf.

———. 2016. 'Digital Identity : Towards Shared Principles For Public And Private Sector Cooperation'. Working Paper 107201. World Bank Group. https://documents1.worldbank.org/curated/en/600821469220400272/pdf/107201-WP-PUBLIC-WB-GSMA-SIADigitalIdentity-WEB.pdf.

———. 2018a. 'Privacy by Design: Current Practices in Estonia, India, and Austria'. Report. Washington, DC: World Bank. https://documents1.worldbank.org/curated/en/546691543847931842/pdf/Privacy-by-Design-Current-Practices-in-Estonia-India-and-Austria.pdf.

———. 2018b. 'Private-Sector Economic Impacts from Identification Systems'. Analytical Report. Washington, DC: World Bank. https://documents.worldbank.org/en/publication/documents-reports/documentdetail/739851531204180818/private-sector-economic-impacts-from-identification-systems.

———. 2018c. 'Technology Landscape for Digital Identification'. Washington DC: The World Bank. https://documents1.worldbank.org/curated/en/199411519691370495/Technology-Landscape-for-Digital-Identification.pdf.

———. 2019. 'ID4D Practitioner' Guide: Version 1.0'. Version 1.0. Washington DC, United States: The World Bank. https://documents1.worldbank.org/curated/en/248371559325561562/pdf/ID4D-Practitioner-s-Guide.pdf.

———. 2021a. ‘Digital ID to Enhance Financial Inclusion: A Toolkit for Regulatory Authorities’. Toolkit / Guidance Report. Washington, DC: World Bank Group. https://documents.worldbank.org/en/publication/documents-reports/documentdetail/210151633568180162/digital-id-to-enhance-financial-inclusion-a-toolkit-for-regulatory-authorities.

———. 2021b. ‘ID4D Global Dataset 2021’. Global ID Coverage. 2021. https://id4d.worldbank.org/global-dataset#highlights.

———. 2022. *National Digital Identity and Government Data Sharing in Singapore*. Washington, DC. https://doi.org/10.1596/38201.

———. 2023. ‘Putting People at the Center of Digital Public Infrastructure (DPI): Annual Report 2023’. Text/HTML. World Bank Group. 2023. https://documents1.worldbank.org/curated/en/099647503042425828/pdf/IDU-a9d1a6be-30dc-48e6-9318-cf9d26959fb9.pdf.

———. 2025a. ‘Ayushman Bharat Digital Mission’s Integrated Digital Health Ecosystem’. Case study / Technical Report. Washington, DC: World Bank. https://documents.worldbank.org/en/publication/documents-reports/documentdetail/387191704302435431/ayushman-bharat-digital-mission-s-integrated-digital-health-ecosystem.

———. 2025b. ‘Digital Public Infrastructure and Development: A World Bank Group Approach. Digital Transformation White Paper, Volume 1’. Volume 1. Washington DC, United States: The World Bank. https://documents1.worldbank.org/curated/en/099031025172027713/pdf/P505739-84c5073b-9d40-4b83-a211-98b2263e87dd.pdf.