DPI

DIGITAL PUBLIC INFRASTRUCTURE AND DEVELOPMENT: A WORLD BANK GROUP APPROACH

DIGITAL TRANSFORMATION
WHITE PAPER, VOLUME 1

MARCH 2025

WORLD BANK GROUP

ID4D

G2Px

PROJECT FAST
FRICTIONLESS • AFFORDABLE • SAFE • TIMELY • TRANSACTIONS

1818 H Street NW, Washington DC 20433
Telephone: +1-202-473-1000
Internet: www.worldbank.org

Attribution

Please cite the work as follows: "Clark, J., Marin, G., Ardic Alper, O.P., Galicia Rabadan, G.A. 2025. Digital Public Infrastructure and Development: A World Bank Group Approach. Digital Transformation White Paper, Volume 1. © Washington, DC: World Bank."

TABLE OF CONTENTS

List of Figures

List of Tables

List of Boxes

ACKNOWLEDGEMENTS

This paper was prepared by Julia Clark, Georgina Marin, Oya Pinar Ardic Alper, and Guillermo Alfonso Galicia Rabadan. Clément Gevaudan and Aishwarya Viswanathan prepared the additional country examples published in Volume 2 of this paper and referenced throughout.

Many World Bank Group colleagues contributed important inputs to both volumes of this series, including Mohamed Almenfi, Boniface Okelo Akuku, Saniya Ansar, Karina Baba, Holti Banka, Adele Moukheibir Barzelay, Gunhild Berg, Luda Bujoreanu, Leyla Castillo, Luciano Charlita De Freitas, Nay Constantine, Stephen R. Davenport, Francesco Di Salvo, Marie Eichholtzer, Anette Bayer Forsingdal, Jacob Gahamanyi, Marelize Gorgens, Melis U. Guven, Sylvan Herskowitz, Serene Ho, Matthew Hulse, Abdallah Jabbour, Johanna Jaeger, Tim Kelly, Lewis Malike Kendeh, Zaki Khoury, Liana Korkotyan, Parvathy Krishnan Krishnakumari, Victor Kyalo, Claudio Machado, Viky Manaila, Jonathan Marskell, Ida S. Mboob, Claudia Carlisle Meek, Anna Metz, Andrea Monteleone, Ivan Mortimer-Schutts, Julian Najles, Marco Nicoli, Etkin Ozen, Maria Claudia Pachon, Nidhi Sunil Parekh, Thomas Piveteau, I Gede Putra Arsana, Nilima Ramteke, Douglas Randall, Marlon Rolston Rawlins, Constantin Rusu, Marc Schrijver, Kateryna Schroeder, Parmesh Shah, Arun Sharma, Venkat Bhargav Sreedhara, Maletela Tuoane, Christopher Tullis, Minita Varghese, Goran Vranic, Ambrose Wong, and Siegfried Zottel.

The authors also wish to thank Ami Dalal, Spyridon Demetriou, and Harish Natarajan (World Bank); Kamya Chandra, Dan Abadie, and Tanushka Vaid (Center for DPI); Sarah Fischer (GovStack); Robert Opp and Keyzom Ngodup (UNDP); and Ana María Prieto (Central Bank of Colombia) for their valuable peer reviews and comments. Furthermore, this paper benefited greatly from earlier guidance and reviews provided by Christine Qiang, Peter Kusek, Harish Natarajan, Arturo Gutierrez, Arianna Legovini, Robin Mearns, Jean Pesme, Carlo Rossotto, Sofie Sirtaine, and Juan Pablo Uribe. The initial concept for this paper was developed by the cross-department Directors and Working Groups for the World Bank Group's Identification and Development (ID4D) and Digitizing Government-to-Person Payments (G2Px) Initiatives.

ABOUT

ID4D

The World Bank Group's Identification for Development (ID4D) Initiative uses global knowledge and expertise across sectors to help countries realize the transformational potential of digital identification (ID) systems to achieve the Sustainable Development Goals. It operates across the World Bank Group with units working on digital transformation, social protection, health, financial inclusion, agriculture, governance, gender, legal, and research, among others. The mission of ID4D is to enable all people to access services and exercise their rights, by improving the inclusivity, design, and governance of ID and civil registration (CR) systems. ID4D makes this happen through its three pillars of work: (1) thought leadership and analytics to fill knowledge gaps; (2) global convening and networks to amplify good practices; and (3) country and regional action to support the implementation of trusted, inclusive, and responsible ID and CR systems. The work of ID4D is made possible with support from the World Bank Group, Gates Foundation, UK Government, French Government, Norwegian Agency for Development Cooperation, and Omidyar Network. To find out more, visit id4d.worldbank.org.

G2PX

The World Bank Group's G2Px (Digitalizing Government-to-Person Payments) Initiative focuses on transforming government-to-person (G2P) payments to accelerate development outcomes, including financial inclusion, women's economic empowerment, resilience, and government-wide efficiency gains. G2Px supports countries in modernizing their G2P payment ecosystems with recipient-centric frameworks and evidence-based guidance on sustainable and inclusive models. G2Px works through three reinforcing pillars of work: (1) thought leadership and analytics to build evidence and develop guidance; (2) country action to support countries in their modernization of G2P architectures; and (3) global convening and networks to share good practices. G2Px operates across the World Bank Group with units working on digital transformation, social protection, agriculture, health, financial inclusion, payment systems, social inclusion, governance, research, gender, and data protection, among others. The work of G2Px is made possible with the support from the World Bank Group, Gates Foundation, Norwegian Agency for Development Cooperation, and French Government. To find out more, visit www.worldbank.org/g2px.

PROJECT FASTT

The World Bank is committed to accelerating the global adoption of Fast Payment Systems (FPS) through Project FASTT (Frictionless Affordable Safe Timely Transactions). Project FASTT focuses on the role and features of FPS, aiming to produce knowledge and provide technical assistance that centers on creating dynamic and interoperable systems facilitating financial inclusion. FASTT aims to accelerate implementations of FPS across the world, but also to create an enabling environment to promote usage (such as, conducive regulatory framework, value-added services such as QR codes and alias registries, consumer protection and fraud mitigation, and so on). Project FASTT is also intrinsically synergistic with ID4D, G2Px, and other initiatives, including collaboration with the World Bank Development Economics (DEC) on randomized studies to measure the impact of FPS on financial inclusion and women's empowerment. The Project encompasses four main areas of activity: (1) data and research, (2) dissemination and advocacy, (3) capacity building, and (4) technical assistance and lending operations. The work of Project FASTT is made possible with support from the Gates Foundation. To find out more, visit fastpayments.worldbank.org.

ABBREVIATIONS

ACH	Automated Clearing House
AI	Artificial Intelligence
API	Application Programming Interface
B2G	Business to Government
BIS	Bank for International Settlements
CDPI	Center for Digital Public Infrastructure
CSO	Civil Society Organization
DGPA	Digital Public Goods Alliance
DGS	Digital Government Services
DPI	Digital Public Infrastructure
EMDE	Emerging Markets and Developing Economies
FASTT	Frictionless Affordable Safe and Timely Transactions
FMI	Financial Market Infrastructure
FPS	Fast Payment System
G2P	Government to Person
G2Px	Digitalizing Government to Person Payments Initiative
GCP	Global Challenge Program
GPFI	Global Partnership for Financial Inclusion
GRM	Grievance Redress Mechanism
HCD	Human-Centered Design
IADB	Inter-American Development Bank
ID	Identification
ID4D	Identification for Development Initiative
IDP	Identity Provider
ISO	International Organization for Standardization
LRIs	Laws, Regulations, and Institutions
MIS	Management Information System
ML	Machine Learning
OECD	Organization for Economic Co-operation and Development
OSS	Open-Source Software
P2G	Person to Government
P2P	Person to Person
PFMIs	Principles for Financial Market Infrastructures
PSP	Payment Service Provider
RP	Relying Party
SOGI	Sexual Orientation and Gender Identity
SSI	Self-Sovereign Identity
UNCITRAL	United Nations Commission on International Trade Law
UPI	Unified Payments Interface
VCs	Verifiable Credentials
WB	World Bank
WEE	Women's Economic Empowerment

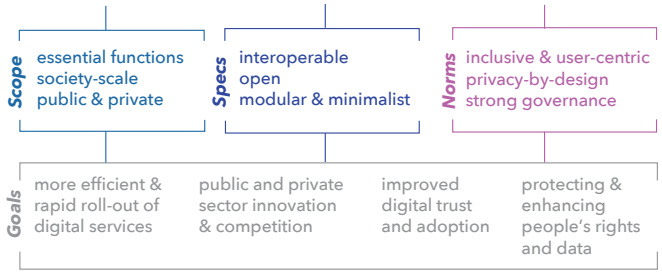
EXECUTIVE SUMMARY

This paper presents a one-World Bank Group (WBG) framework for understanding and implementing Digital Public Infrastructure (DPI) to accelerate safe and inclusive digital transformation.

DPI is an approach to digitalization focused on creating "foundational, digital building blocks designed for the public benefit." By providing essential digital functions at society scale that can be reused across sectors, DPIs enable public and private service providers to build on these systems, innovate, and roll out new services more quickly and efficiently. Common systems built as DPIs include digital identity and electronic signatures, digital payments, and data sharing. However, to provide DPI functionality, these systems must embed principles such as inclusion, openness, modularity, inclusivity, user-centricity, privacy-by-design, and strong governance.

World Bank Definition of Digital Public Infrastructure

Foundational, digital building blocks for the public benefit.

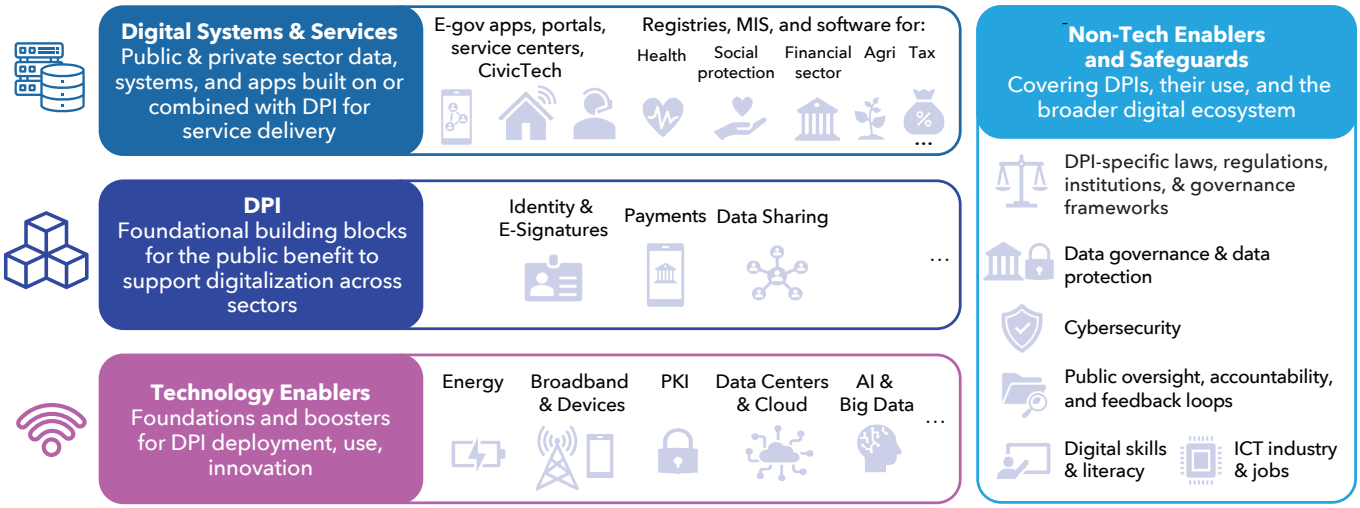


DPIs are part of a broader digital ecosystem and encompass much more than technology. Although DPIs can be a key accelerator for digital transformation, they do not exist in isolation. They rely on various other technology enablers, such as broadband connectivity, devices, and data centers and cloud, along with the digitalization of systems across sectors. This often involves close integration with digital public service channels and platforms such as e-service applications; however, in contrast to typical e-government approaches, DPI can be provided both by the public and private sector. Furthermore, successfully developing and deploying DPIs requires broader ecosystem enablers, including whole-of-society digital transformation strategies; legal and regulatory frameworks for data governance, protection, and e-transactions; strong cybersecurity capacity; sound governance and oversight; and efforts to build digital literacy and skills across the public and private sector.

The DPI approach differs from traditional digitalization efforts in a few ways, though there is no single model or blueprint for implementing DPI. DPI emphasizes shared, reusable building blocks, fostering whole-of-society collaboration—including strong involvement from the private sector—and embedding core principles such as openness, interoperability, data protection, and user choice. This contrasts with the fragmented approach where each sector develops its own isolated digital systems, leading to redundancy, inefficiency, high costs. Implementing this approach in practice will look different in each country or jurisdiction. Regardless of the model adopted, however, DPI requires strong and sustained political commitment, meaningful and frequent stakeholder engagement, institutional and technical capacity, and comprehensive legal and regulatory frameworks, among other success factors.

The COVID-19 pandemic underscored the value of DPI, demonstrating that countries with existing DPIs were able to deliver emergency assistance faster and more effectively. A DPI approach—and specific DPIs themselves—offer multiple potential benefits. For example, the availability of high-quality shared digital building blocks can significantly improve efficiency and reduce costs of government and private sector service providers, accelerating the development of new services. It can also enable significant private sector innovation and competition, potentially further improving service quality and

Broader DPI Ecosystem



efficiency, and helping to develop new services, developer communities, and digital markets. By providing systems that focus on inclusion, public accountability, data privacy and protection, and user control, DPI's public benefits orientation can improve consumer experiences and empowerment, the quality of services and data, and online trust and security. Examples of potential benefits across sectors include:

- **Government-to-person (G2P) payments:** Faster, more efficient, and inclusive delivery of social benefits, reducing costs and leakages.
- **Financial inclusion:** Increased access to financial services, particularly for marginalized populations, through reduced costs and improved accessibility.
- **Health:** Improved healthcare delivery, disease surveillance, and public health interventions through interoperable health information systems and secure payments.
- **Agriculture:** Enhanced access to services, data-driven decision-making, climate resilience, and efficient markets for farmers.

However, there are also important challenges and risks associated with DPI implementation:

- **Legacy systems:** Overcoming institutional inertia and integrating DPI with existing systems.
- **Inclusion and the digital divide:** Addressing gaps in connectivity, device access, and digital literacy, and ensuring accessibility of DPI for marginalized and vulnerable groups.
- **Data privacy and protection:** Ensuring robust safeguards to protect personal data and user rights.
- **Cybersecurity:** Mitigating operational risks and cyber threats.
- **Deployment and procurement:** Avoiding lock-in and ensuring effective contract management and sustainability over time.

Successful DPI implementation requires a multi-faceted approach:

- **Prioritizing safety and inclusion:** Embedding data protection, security, and accessibility into the design of DPI systems. This includes robust legal and regulatory frameworks, privacy-enhancing technologies, and proactive engagement with civil society organizations (CSOs).
- **Focusing on outcomes, not technology:** Adopting a use-case or service-design approach, starting with a thorough assessment of needs and prioritizing impactful applications. This requires stakeholder consultations, data-driven decision-making, and regular feedback loops.
- **Putting users at the center:** Employing human-centered design (HCD) principles throughout the DPI lifecycle,

including user research, co-creation, prototyping, piloting, and iterative design. This ensures that DPIs are user-friendly, accessible, and meet the needs of diverse populations.

- **Investing in people:** Building capacity within government, the private sector, and among citizens through training and digital literacy programs. This is crucial for the long-term sustainability and effectiveness of DPI initiatives.
- **Adopting a whole-of-society approach:** Fostering collaboration among government agencies, the private sector, CSOs, and other stakeholders. This includes establishing clear roles, responsibilities, and coordination mechanisms.

By leveraging the opportunities presented by DPI, countries can accelerate their digital transformation journeys and achieve more inclusive and sustainable development. The World Bank Group is committed to supporting this crucial endeavor. The WBG's new Global DPI Program will address key knowledge gaps and support countries in building safe, inclusive, and transformative DPI.

INTRODUCTION

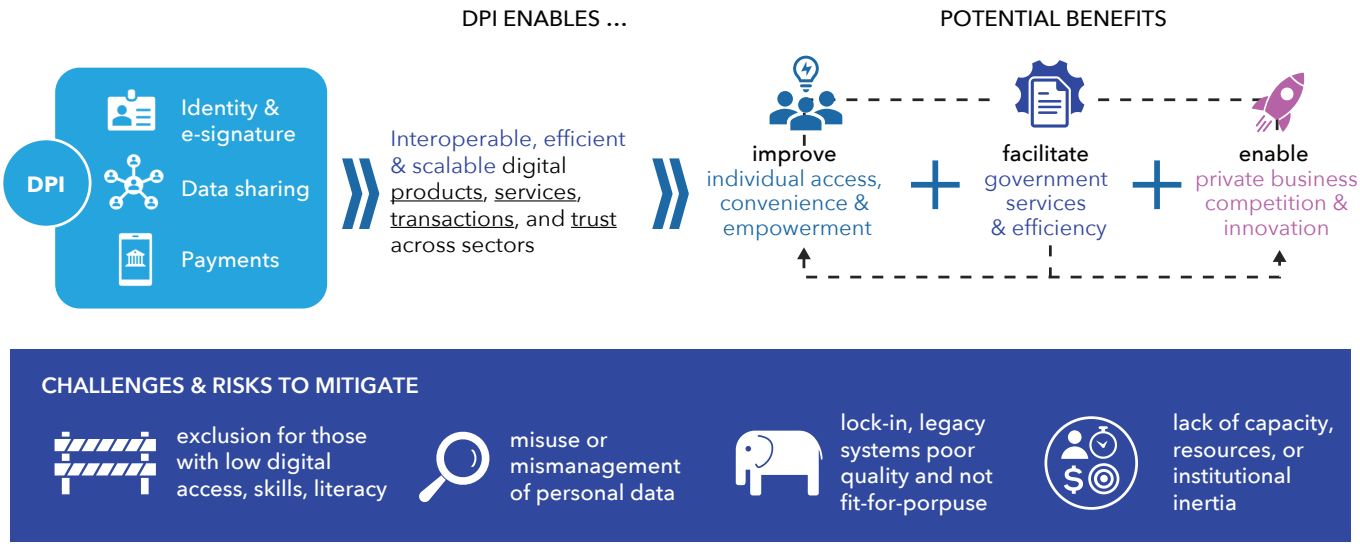
"With a few taps on their mobile phone, remote area workers in India can **apply for social benefits** to be paid directly into their bank account and electronically sign an application for a loan. In Thailand, farmers can **receive fertilizer subsidies into a bank account** linked to their identification (ID). In Singapore citizens and residents can conduct almost **any transaction end-to-end online**, no matter where they are, from registering a birth to filing taxes and opening a new business. **These services are made possible through innovations catalyzed by digital public infrastructure.**" – World Bank (2024a).

1. MOTIVATION

Digital public infrastructure (DPI) is an emerging approach to achieve fast, efficient digital transformation at scale. It involves developing essential digital capabilities or DPIs—such as digital identity verification, payments, and trusted data sharing—that are required for many digital services and transactions across the public and private sector. By providing these systems as interoperable and modular building blocks that can be easily integrated into a variety of software applications and processes, DPI enables governments and firms to rapidly deploy new or improved services, rather than reinventing the wheel for each new application (Desai et al. 2023). The ability of interoperable DPI services to work together as a "digital stack" facilitates a variety of use cases—for example, across sectors such as financial services, healthcare, agriculture, and social protection—and allows for streamlined, on-demand, and paperless transactions, reducing costs and spurring innovation and new markets (World Bank 2022a, CDPI 2024). DPI can support broader digital transformation strategies, including those focused on building digital public services and digitalization across sectors. It also offers a central role for the private sector as DPI providers and users, creating new opportunities for crowding private investment into the digital service ecosystem. Finally, a DPI approach embeds principles around inclusion, data protection, and user-centricity, and advocates for strong safeguards to ensure that no one is left behind.

The utility of this approach became evident during the COVID-19 pandemic and subsequent wave of momentum around digitalization. During the pandemic, countries with existing DPIs were able to provide emergency assistance faster and reach three times more beneficiaries, compared to countries without (World Bank 2022b). In **Thailand**, for example, the ability to link a digital ID to a bank or e-wallet account enabled informal workers to complete an online application for an emergency cash transfer quickly and conveniently, and then receive payment directly in their account (World Bank 2024a). The pandemic accelerated recognition of DPI's value proposition for scaling digital transformation faster and more efficiently. This prompted international collaboration and consensus on DPI standards, notably through the G20 agreement on guiding principles for DPI (World Bank 2024a). This momentum has been supported by global organizations like the World Bank Group (WBG), United Nations (UN), Organization for Economic Cooperation and Development (OECD), Digital Public Goods Alliance (DPGA), Gates Foundation, Center for Digital Public Infrastructure (CDPI), Digital Impact Alliance (DIAL), Co-Develop, and GovStack, among others, that have prioritized DPI as a crucial enabler of digitalization for sustainable development.

Figure 1. Key benefits and challenges of DPI



Source: Original figure for this paper.

However, challenges and risks remain in deploying and utilizing DPI effectively. As summarized in Figure 1, these include legacy digital platforms (such as digital identity, payments, data sharing) that lack the interoperability, modularity, security or inclusivity to play the role of DPI; incomplete or inaccurate foundational identification (ID) and civil registration systems to provide trusted identity data; low institutional and technical capacity or resources; poor underlying digital data quality and accuracy; inadequate data governance, protection, and other safeguards that are critical to fostering trust; exclusion or discrimination in access to digital systems; and deficits in internet and device access and affordability to ensure everyone can take advantage of digital opportunities (World Bank & IADB 2024). Addressing these issues is crucial to fully realizing the potential of a DPI approach to enhance public service delivery, stimulate innovation, build digital trust, and close the divide in digital adoption.

The WBG supports countries to overcome these challenges and achieve safe, inclusive, and transformational digitalization through DPI linked to high-impact services. Through its Identification for Development (ID4D) Initiative, the WBG is providing technical assistance and/or financing for nearly 70 countries to develop safe and inclusive digital ID and civil registration systems that can be leveraged as DPI. Moreover, the World Bank recently launched Project FASTT (Frictionless Affordable Safe Timely Transactions) to work on the nexus of digital payments and financial inclusion, produce knowledge, and provide technical and financing assistance for implementing fast payment systems (FPS). From a use case perspective, the Digitalizing Government-to-Person Payments (G2Px) Initiative focuses on leveraging DPI to help modernize the delivery of government benefits to improve convenience, financial inclusion, and women's economic empowerment (WEE).[1]

As this approach has gained momentum, the WBG has further prioritized DPI and safeguards as key elements of digital transformation. For example, safe and inclusive DPI is one of three priority investment areas under the Accelerating Digital Global Challenge Program (GCP), which provides targeted support to boost digital inclusion and service delivery over the next five years. Similarly, DPI and safeguards are part of the digital policy commitment under IDA21, which will support low-income countries to invest in digital infrastructure. A new Global DPI Program will provide a one-WBG approach to public and private sector investments that support and safeguard DPI as a key ingredient to delivering digital services at scale.

1 For more information on ID4D, G2Px, and Project FASTT, see http://id4d.worldbank.org, https://www.worldbank.org/en/programs/g2px, and https://fastpayments.worldbank.org/, respectively.

2. PURPOSE & SCOPE

This paper provides a common framework and primer on DPI for policymakers, practitioners, WBG staff, and the broader development community. It builds on existing work, including the World Bank's Digital Progress and Trends Report (World bank 2024a), World Development Reports on digital and data (World Bank 2016 & 2021a), and other related efforts. Specifically, this paper outlines:

- **DPI Concepts and Theory of Change:** This includes a working definition of DPI and its core characteristics, including the role of the private sector, how DPI differs from past approaches to digitalization, and the relationship between core DPI systems, sector-specific systems, other digital technologies, and broader ecosystem enablers and safeguards. The paper also articulates the potential benefits of DPI across a range of public and private sector services, and risks and challenges for implementation and adoption.
- **Considerations for Implementation:** Drawing on the experiences of a diverse set of countries across regions, income levels, and DPI approaches, the paper identifies common trends for building, scaling, and using DPIs that are safe and inclusive. This includes identifying what we know (and do not yet know) around different DPI design choices and models, implementation strategies, procurement, issues around use case integration and sequencing of DPI, and more.
- **Principles and Practical Lessons:** Finally, it summarizes key lessons from countries' experiences with DPI to date, highlighting critical success factors and risk mitigation strategies for policymakers, practitioners, and development partners. A separate volume provides examples of DPI from countries around the globe.

In terms of scope, this paper focuses on high-level considerations for building and using DPI. While it discusses systems like digital identity, payments, and data sharing that can be built as DPIs, it does not provide in-depth technical details on how to implement each of these systems or any specific DPI use case. For identity, payments systems and related use cases, there is already a deep body of technical guidance from ID4D, Project FASTT, and G2Px, which can be found online.[2] Newer topics, including data sharing, e-signatures, and DPI use cases beyond G2P payments are treated more lightly in the paper but will be the subject of future work under the WBG Global DPI Program. Finally, DPI does not exist in isolation and is closely linked to other digital technologies and various government and private sector systems and applications. This broader ecosystem is summarized in Section 2; however, an in-depth treatment of these complementary topics is outside the scope of this paper.

3. ORGANIZATION

This paper is organized as follows: Section 2 outlines the WBG working definition of DPI and the broader DPI ecosystem, including core DPI systems, sector-specific digital systems, technology enablers, and DPI governance, enablers, and safeguards. It also provides a deep dive into why and how DPI can be a key enabler of digital transformation across sectors, along with specific risks and challenges to DPI implementation, including those related to inclusion, data protection, institutional inertia, legacy systems and procurement challenges, and more. Section 3 draws on the country case studies included in Volume 2 of this series to outline key trends in DPI implementation, including core design choices and models, implementation questions, and use case integration. Section 4 outlines important lessons learned to date for successfully building and using DPI. Finally, Section 5 highlights key areas where additional work is needed that will be the focus of the WBG's new Global DPI Program.

2 See, for example, the ID4D Practitioner's Guide (http://id4d.worldbank.org/guide), Project FASTT's Flagship Report (https://fastpayments.worldbank.org/), and G2Px Modern G2P Architecture (https://www.worldbank.org/en/programs/g2px).

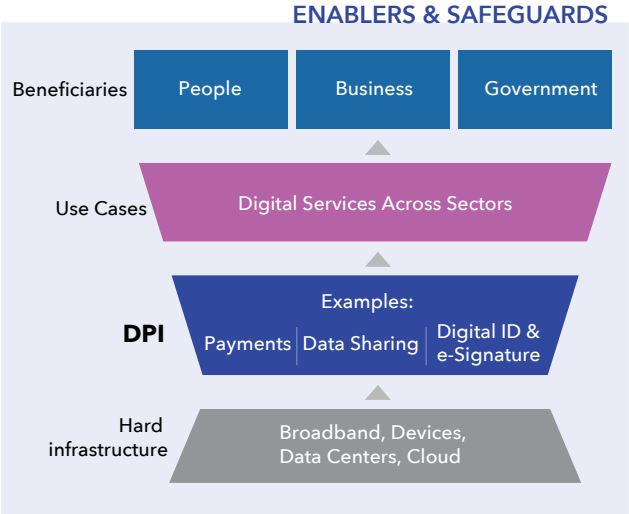
II UNDERSTANDING DPI

What is DPI, and why does it matter for development? This section builds a working definition of DPI and its core characteristics and explains why it represents a new approach to digitalization that prioritizes common infrastructure, inclusion, and trust. It also provides a framework for thinking about DPI in relation to the broader digital ecosystem, clarifying how it relates to hard infrastructure, other new technologies, broader digital government services, and sector-specific digital systems while outlining governance requirements and other enablers and safeguards. Finally, it provides a concise theory of change for DPI, identifying how and when it can have positive impacts across sectors, as well as associated challenges and risks.

1. DEFINING DPI

DPI is a relatively new approach to digitalization that focuses not only on what to build, but on how to build it for scale, impact, and safety. Specifically, it represents shared digital resources that are designed for the public benefit and can be reused across sectors to avoid reinventing the wheel for each new digital service. At its simplest, DPI can be understood as an intermediate software layer in the digital ecosystem that sits atop physical infrastructure (including internet connectivity, devices, servers, data centers, and cloud) and below the layer of platforms and applications that leverage DPI building blocks to deliver specific services. These may include integrated portals for accessing digital public services, e-commerce platforms, telemedicine services or electronic health records systems, and more (see Figure 2).

Figure 2. DPI: Between hard infrastructure and service applications



Source: Adapted from World Bank (2024).

This overall vision for DPI is generally shared across prominent global actors, though there are important variations in each organization's interpretation of DPI and areas of emphasis (see Box 1). CDPI, for example, considers DPI as an approach to harnessing digital technology for social change that must adhere to a discrete set of technical architecture principles around interoperability, minimalism, innovation, inclusion, decentralization, security, and privacy (CDPI 2024).[3] The earlier G20 framework (G20 2023a) includes many of the same characteristics and further emphasizes the need for clear governance and community components of DPI in addition to technology.[4] The G20 and the Global Partnership for Financial

3 The CDPI architecture principles include interoperability driven by open specifications; minimalist, reusable building blocks; diverse, inclusive, innovation by the public and private ecosystem via open and multimodal access; federated and decentralized with a preference for letting data stay where it is collected; and security and privacy by design (CDPI 2024a).

4 G20 Digital Economy Working Group (DEWG) framework from August 2023 includes the following suggested principles for DPI: inclusivity; interoperability; modularity and extensibility; scalability; security and privacy; collaboration; governance for public benefit, trust, and transparency; grievance

Box 1. Example DPI definitions

G20 Digital Economy Working Group (DEWG): "set of shared digital systems that should be secure and interoperable, and can be built on open standards and specifications to deliver and provide equitable access to public and / or private services at societal scale and are governed by applicable legal frameworks and enabling rules to drive development, inclusion, innovation, trust, and competition and respect human rights and fundamental freedoms" (G20 2023a).

G20 Global Partnership for Financial Inclusion (GPFI): "interoperable, open, and inclusive systems supported by technology to provide essential, society-wide, public and private services" (Ardic Alper et al., 2023).

GovStack and Digital Public Goods Alliance (DPGA): "solutions and systems that enable the effective provision of essential society-wide functions and services in the public and private sectors. This includes but is not limited to digital forms of ID and verification, civil registration, payment (digital transactions and money transfers), data exchange, and information systems (including sector-specific, i.e., health or education). A country's digital public infrastructure may include implementations of multiple proprietary and/or open-source solutions (including digital public goods)" (GovStack Community of Practice 2022).

OECD: "common, foundational digital systems that enable the delivery of services in the digital age. Elements of DPI can be developed by the public or private sector, or co-developed to benefit the delivery and access to services across both sectors, and eventually across borders. DPI needs to be standards-based and re-usable" (OECD 2024).

Center for Digital Public Infrastructure (CDPI): "an approach to solving socio-economic problems at scale, by combining minimalist technology interventions, public-private governance, and vibrant market innovation" (CDPI website).

Note: Adapted from World Bank & IADB (2024).

Inclusion (GPFI) consider DPIs to be interoperable, open, and inclusive systems supported by technology that facilitate essential services for society, and that encompass protocols, frameworks, and governance structures utilized by market players to serve customers (Ardic Alper et al. 2023).[5] Nearly all definitions recognize digital identity, digital payments, and data sharing as examples of systems that can be built as "core" DPIs, while allowing for flexibility in the emergence of additional essential building blocks, and in each country's approach to establishing its own DPI.

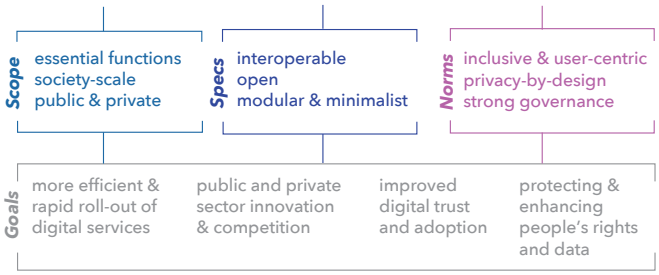
Building on the above work, this paper develops a common definition of DPI across the WBG that attempts to further distill these concepts into a simple and practical framework. To be useful, this definition should resonate with policymakers and practitioners across diverse country contexts and allow for flexibility as this new concept evolves over time. This requires avoiding a definition that is too specific or rigid to be useful, or too general such that the term essentially becomes meaningless (Porteous 2023). The definition below attempts to strike this balance by articulating a short definition that embodies and organizes the primary characteristics or principles of DPI.

redress; sustainability; human rights; intellectual property protection; and sustainable development (G20 2023a).

5 This document was prepared by the World Bank as an implementing partner of the GPFI, with inputs from the GPIF members and other GPFI implementing partners.

World Bank Group Definition

Figure 3. Defining DPI at the World Bank Group



Source: Original figure for this publication.

Digital public infrastructure (DPI) refers to systems that serve as foundational, digital building blocks for public benefit (Figure 3). Systems built as DPI can comprise a variety of digital software, platforms, APIs, and services, along with their related legal and regulatory frameworks, standards, policies, and processes. The term "DPI" can refer to this overall approach or to the set of specific systems built as DPIs within a country. Unpacking this definition highlights the essential characteristics or principles of DPI(s):

- **Foundational:** DPIs provide essential digital functions or resources at society scale—that is, not limited to a particular sector or population—enabling widespread adoption by government, firms, and individuals. Crucially, DPIs can be provided by the public and/or private sector. While each country takes a different approach to identifying and defining these essential functions, common examples of foundational systems include—but are not necessarily limited to—those that provide digital identity and e-signatures, digital payments, and data sharing.
- **Building Blocks:** A building block design enables DPIs to be adopted and reused across institutions, applications, sectors, and borders. This requires them to be open and interoperable, including the use of open standards and open specifications. In addition, a modular and minimalist design allows DPIs to provide a discrete set of functions that can be integrated into diverse services with minimal disruption, while avoiding unnecessary centralized data storage or processing.
- **For the Public Benefit:** DPI is a developmental approach that requires embedding principles around inclusion and user centricity (for example, user choice, control, and accessibility); privacy-by-design; and strong governance including public oversight and accountability, to achieve the promise of safe and trusted digitalization that leaves no one behind. While DPIs also require external safeguards, these norms should be embedded into the technical design of DPIs by default.

When built for the public benefit, these foundational, digital building blocks can achieve multiple goals. By providing essential digital tools that can be reused and integrated into a variety of digital applications, the soft infrastructure of DPI can underpin the rapid development and deployment of trusted digital services and catalyze innovation across the economy. DPI's public benefit orientation—which emphasizes user centricity, inclusivity, privacy –by design, and transparent governance—and helps to avoid common digital pitfalls by protecting users' rights and data, and boosting digital trust, adoption, and competition.

Importantly, many countries already have well-functioning digital systems that provide many benefits but do not fully meet this ideal-type definition of DPI. This is particularly the case for countries that were early adopters of digital solutions and platforms, as certain practices—such as interoperability, the use of open standards, privacy-enhancing technologies, and user control—have developed rapidly over the past 5-10 years. In such cases, moving toward a DPI approach may involve some gradual reforms to already operational and valuable systems, rather than building new systems from scratch. The goal of this definition is not to imply that only those systems that meet all DPI criteria are "good." Rather, it is to highlight important DPI principles and provide direction for how current systems can evolve to fully realize the potential of society-scale digitalization, platforms, and services.

Finally, DPI is distinct from—but complements—broader digital public services or sector-specific digital data or infrastructure, such as government e-serviceportals, e-gov applications; digital registries for social protection, business, credit, agriculture; health-sector interoperability and data exchange standards; information systems for digital tax or human resources, and so on. DPIs do not replace such systems, but rather help enable and scale other digital services and platforms more quickly, reliably, and efficiently. The following section unpacks these characteristics in more detail.

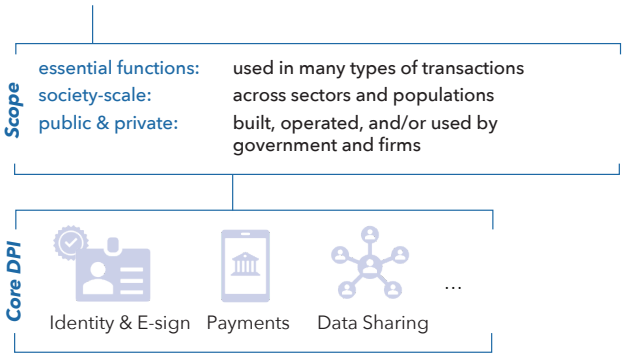
Foundational

The "foundational" nature of DPI relates to its scope, answering the question: *What kinds of systems could be a DPI?*

To provide soft infrastructure that is relevant for the public at large, core DPIs must be relevant to many types of transactions, population groups, and sectors. For example, the GPFI distinguishes between other financial infrastructure (such as credit reporting systems and automated clearing houses) and DPIs based on their "cross-sectoral nature and use across a wide range of economic and social interactions" (Alper et al. 2023, p. 2). As noted in Figure 4, examples of systems that commonly meet these foundational criteria include those that facilitate identity verification and authentication, digital payments, and data sharing. However, a recent paper on DPI in Latin America and the Caribbean notes that the nature of what is considered essential and available at society scale can be a matter of degrees, and the scope of DPI requires flexibility to adapt to context (World Bank & IADB 2024). Each country may arrive at its own definition of what core functions are foundational for its digital ecosystem.

Furthermore, this sector-agnostic characteristic of DPI does not mean that digital systems or resources within a specific sector cannot be built with "DPI thinking."[6] Even if a system designed for a narrower purpose does not meet the foundational scope criteria of DPI, it could still follow the DPI specifications and norms discussed below—such as interoperability, modularity, user-centricity, and privacy-by-design—to enable public benefit and innovation. In **Kenya**, for example, an agriculture-specific data platform has focused on interoperability and user centricity, with the goal of building a resource that can be used by different players across the sector (see Box 2).

Figure 4. Foundational characteristics of DPI



Source: Original figure for this publication.

Box 2. Kenya's Big Data Platform for agriculture

In Kenya, the Big Data Platform at the Kenya Agricultural and Livestock Research Organization (KALRO), supported by the World Bank, was designed with "infrastructure thinking" that embraced many DPI characteristics at the sector level.

Rather than focusing on technology solutions, it involved a holistic approach to understanding and improving systems and emphasizing the interoperability and interconnectedness of components within the big data ecosystem (Makini et al 2020). The fundamental design principles included a farmer service-oriented perspective, sustainability (future-ready technology), adaptability, and collaboration with the one-farmer platform ag-tech startups. Applying these principles not only has benefits for the agriculture sector but enables future integration with Kenya's DPI to enhance potential impact.

The Kenyan Big Data Platform now hosts 6.5 million farmers and a geo-tagged digital registry of farms. It has enabled millions of users access diverse digital services, and has fostered several innovations, including location-crop-growth-stage specific digital climate advisory services, crop-livestock-pasture selector, and digitized Good Agricultural Practices (GAP) advisory services. The Big Data Platform is the backbone for delivering essential digital public agricultural services, unlocking groundbreaking innovation for farmers, agribusinesses, investors, and policymakers in the Kenyan agricultural ecosystem, and demonstrating impact and scale in digital service delivery in the sector.

6 See CDPI. "DPI Thinking" Retrieved on 8 August 2024 from https://docs.cdpi.dev/the-dpi-wiki/dpi-overview.

In addition to being society-wide in use, the provision of DPI also spans the public and private sector. While the "public" in DPI denotes public benefit (described in more detail below), this does not mean that it must be government-provided. The success of DPI also depends on private sector participation. This includes driving adoption and use through DPI-enabled services, as key innovators in DPI components and technology, and as developers, participants in public-private partnerships (PPP), and DPI providers (World Bank 2024a). Careful attention should be paid to opportunities for crowding in private sector investment in DPI deployment and use and avoiding a regulatory environment that hampers competition and innovation.

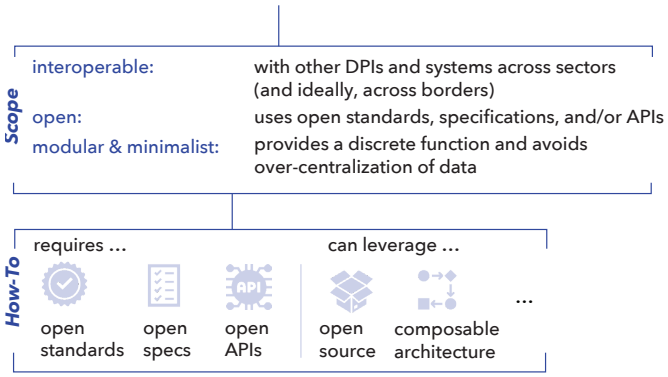
For example, fast payment systems (FPS) typically function as DPIs, providing simplified access and inherent interoperability for digital payments across the economy. The ownership models of FPS can vary, including public, private, and public-private partnerships. For instance, the Banco Central do Brasil, **Brazil's** central bank, crafted a vision for increasing digital payment adoption and implemented this vision by developing Pix. In **India**, the Unified Payments Interface (UPI) is managed by the National Payments Corporation of India, a non-profit company which is an initiative of the Reserve Bank of India (RBI) and the banking association, owned by several banks, payment service operators, payment banks and small finance banks. In **Jordan**, the Cliq and JoMoPay FPS are owned and operated by JoPACC, an entity co-owned by the Jordanian central bank and private banks.

Digital Building Blocks

The characterization of DPI as "digital building blocks" relates to its core specifications, answering the question: *what are the functional design requirements for a DPI?*

To play the role of DPI, foundational systems should be built as interoperable building blocks (see Figure 5). Interoperability is essential to ensure adoption and reuse across the economy; DPIs cannot be fully leveraged unless they can speak to various systems and integrate easily with a diverse set of applications across sectors and potentially across borders. At a minimum, this requires the use of open standards, specifications, and/or APIs, along with clear governance frameworks. To the extent that DPI is open source or built as a digital public good[7] (DPG, see Section 3 for the differences between these concepts),

Figure 5. DPI as digital building blocks



Source: Original figure for this publication.

innovations in one country can more quickly be replicated in others, avoiding the need to repeatedly reinvent the same building block (see for example, the spread of **Estonia's** X-Road solution for data sharing across dozens of countries). Furthermore, the ability of DPI systems to interoperate with each other (that is, to work together as a software stack) creates new possibilities for innovation and seamless service delivery (World Bank 2022a). This approach is leveraged in countries such as **Singapore**, **India**, and **Moldova**.

Although there are many technical specifications and design strategies that can help create building blocks for digitalization, one essential ingredient is openness. This requires open standards, specifications, and application programming interfaces (APIs). One example is Singapore's National Digital Identity (NDI) Stack, which publishes its API specifications, allowing developers to quickly build and test new applications in a sandbox (World Bank 2022a). GovStack[8] provides open, standard-based building blocks that can be utilized across a wide range of use cases, such as identity, registration, messaging, and workflow. **Cambodia** developed its Verify.gov.kh document verification platform using the OpenAttestation open-source software and specifications developed by Singapore's GovTech Agency. In turn, Cambodia is now making its customization of OpenAttestation available to countries such as **Lao PDR** and **Timor Leste**. Newer software design philosophies such as composable architecture, which emphasizes modularity, flexibility, and scalability, and an API-first approach, are also aligned with core DPI goals. This

7 According to the UN and the Digital Public Goods Alliance (DPGA), DPGs are "are open-source software, open standards, open data, open AI systems, and open content collections that adhere to privacy and other applicable best practices, do no harm, and are of high relevance for attainment of the United Nations 2030 Sustainable Development Goals (SDGs)" (GovStack 2022).

8 See https://www.govstack.global/.

is consistent with the overall "building blocks" approach advocated by initiatives such as GovStack.[9]

Finally, building DPIs to be modular and minimalist helps ensure their relevance across applications and their ability to adapt and scale over time with minimal disruption (G20 2023a). Rather than end-to-end solutions, DPIs are akin to small molecules that can be combined and recombined in different ways to create different compounds or services. This is one reason DPIs are often distinct from traditional government service applications, such as e-government service apps or portals . However, DPI and these systems work together hand in hand. For example, **Estonia**'s X-Tee system enables the secure data exchange across different existing platforms, while the e-Estonia platform utilizes this foundation to offer a variety of government services to citizens and businesses. **Moldova** has made significant strides in digitalizing its government-to-business services through the use of shared digital systems, including the M-Connect data exchange platform, and M-Pass and M-Sign for digital identity and e-signatures. **Ukraine**'s Diia app and ecosystem provide multiple DPIs along with a single access point for nearly 120 public services.

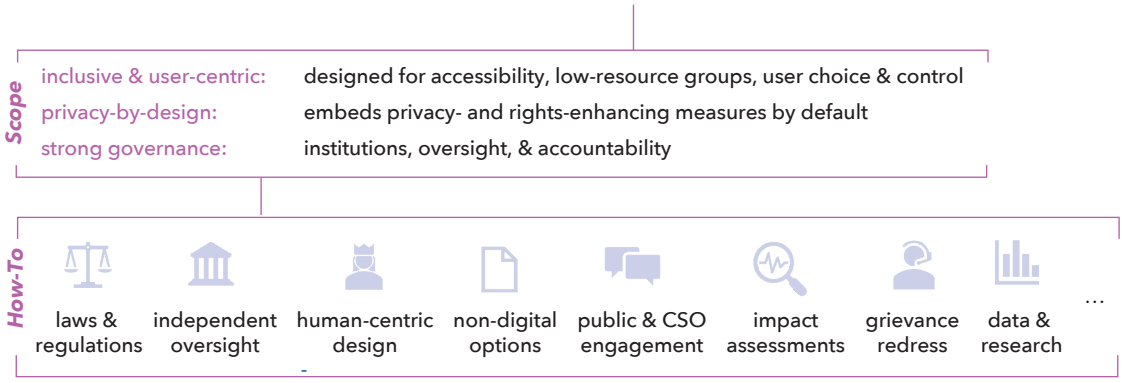
For the Public Benefit

The characterization of DPI as "for the public benefit" relates to the principles it is intended to embody, answering the question: *What are the normative design requirements for DPI?*

Beyond its functional design requirements, the "public" in DPI is commonly understood to denote public purpose and benefit. To have positive impacts for societies—including the attainment of the sustainable development goals (SDGs)—the next wave of digitalization must be rooted in equity, trust, and value (World Bank 2021a) and intentionally designed to serve the needs of people and societies. DPIs can help advance these goals to the extent that they embed core principles required to serve people well, including the most vulnerable in society. This includes strong public oversight and accountability; inherent user centricity that emphasizes convenience and value; putting people in control of their data; ensuring that DPI is universally accessible and addresses the needs of those most likely to be excluded from the digital economy; and embedding technical, legal, and operational controls to ensure that DPI enhances human rights and protects people's privacy by design (World Bank & IADB 2024, G20 2023a, Eaves et al. 2024). While external safeguards (discussed in more detail below) are important, DPI systems should be designed to be inclusive and privacy-protecting by default.[10]

There are myriad tools and strategies available to implement a public benefit orientation in a DPI's technical design and supporting ecosystem. For example, there is a growing trend toward decentralization in digital identity credentials and data sharing—including through verifiable credentials and wallets—to increase user control and reduce the risks associated with centralized data storage. **Korea**, for example, is piloting a new mobile ID (K-DID) using a decentralized, privacy-

Figure 6. DPI for the public benefit



Source: Original figure for this publication.

9 See, for example, the GovStack approach to building blocks here: https://govstack.gitbook.io/specification/building-blocks/about-building-blocks.
10 For example, the UN Office of the Secretary-General's Envoy on Technology (UNOSET) and UNDP have led the development of a DPI safeguards framework that outlines core risks and principles (UNOSET & UNDP 2024). For details, see https://www.dpi-safeguards.org/.

Box 3. What DPI is not: Five common myths

Myth 1. All digital ID, digital payments, and data sharing platforms are DPI. Identity, payments, and data sharing systems all provide critical functions for digitalization. However, many existing systems today do not meet DPI's full scope (for example, they may be limited to a specific sector), functional characteristics (for example, they may not be interoperable and reusable by third parties, and not use open standards or specifications) or norms (for example, they may not incorporate privacy-by-design, user centricity, or other features).

Myth 2. DPI replaces the need for sector-specific digital data or infrastructure. DPI is a complement to sector digitalization, not a replacement. Core sector digital systems and standards—such as digital registries for social protection, business, credit, agriculture; health-sector interoperability and data exchange protocols; a digital tax or human resource management information systems (HRMIS); a government e-service app—are essential investments to be managed in the respective sector. DPIs can help enable and scale sector-owned digital services that rely on these systems more quickly, cheaply, and reliably.

Myth 3. All DPIs require centralization. In some cases, a specific DPI system is operated by a single provider (such as a digital agency that issues an official digital ID credential). However, each DPI often involves different entities, such as a national ID agency, a digital agency, a certificate authority, the central bank, and payment service providers, among others. While data sharing platforms enable data exchange between entities, this does not necessarily involve data aggregation (an exception could be public forms of open data). Indeed, for identity and personal data, there is a significant trend toward federation and decentralization (for example, verifiable credentials and wallets for identity and personal credentials), keeping data where it is collected or in the hands of individual users. Payment systems are by definition centralized. Although new approaches based on distributed ledger technologies could allow for some degree of decentralization, they are not relevant at this point in the context of discussion on DPI.

Myth 4. Building DPI means you must use it for everything. The advantage of DPI is its ability to reuse the same building blocks—such as a fast payments system—for various services such as a health insurance payment, a social welfare benefit, or a person-to-person transfer. However, this does not mean that because a DPI exists, it should be integrated into all services, or that all features of a particular DPI are appropriate in all use cases. For example, high-assurance digital identity services—that is, those that use strong authentication methods such as digital certificates, biometric recognition, and secure devices—may be appropriate for some transactions (such as opening a high-value investment account) but not for others (such as enrolling your child in school online). The goal of a DPI approach is to provide building blocks for innovation and consumer choice, with multiple solutions that can address a variety of service provider and user needs and preferences.

Myth 5. DPI is the end goal or cure-all. DPI is not a silver bullet. It is one piece of a comprehensive strategy for digital transformation, a means to the ends of scaling up impactful digital services and creating new markets that generate benefits for people, governments, and firms. Focusing too narrowly on DPI is likely to be ineffective. Therefore, while the purpose of this paper is to provide a primer on DPI, broader dialogue at the country, regional, and global levels should adopt an outcomes-based approach to digital transformation that considers DPI as part of a broader set of tools and strategies to achieve digitalization goals more quickly and efficiently.

enhancing architecture, as is the **European Union**'s electronic Identification, Authentication and Trust Services or **eIDAS 2.0** scheme, the EU Digital Wallet. Beyond the technology itself, the process of designing and deploying DPIs should follow a multi-stakeholder approach, including consultations with the public and civil society organizations (CSOs),[11] privacy and human-rights impact assessments, regular feedback mechanisms and grievance redress, and ensuring there are non-digital options available for those who need it. Examples of CSO consultations in **Jordan**, **South Africa**, and **Jamaica** are described in more detail in Section 3. Such approaches are essential for building trust in the DPI ecosystem, which is needed for adoption and impact, and to ensure that DPI and its use effectively protects people and their data and helps to close the digital divide.

With regard to digital identity, many modern digital ID systems have sought to minimize data collection and provide individuals with greater control over their information, in line with data protection principles. In **Nigeria**, for example, the National Identity Management Commission (NIMC) is reducing the number of data fields collected for the national ID from over 80 to 10 (Desai & Clark 2021). Countries are also making strides in user agency and convenience through their DPI. In **Indonesia**, the new digital ID application incorporates privacy-by-design features, such as selective disclosure of personal data, allowing individuals to control which specific information is shared, thereby enhancing privacy and security while interacting with government and private sector services. In **Singapore**, the national digital identity platform SingPass has been piloting new user-centric functions such as "digital delegation," which allows citizens to securely and conveniently manage government interactions on behalf of others, addressing the needs of families who previously faced challenges in assisting elderly or overseas relatives.

Finally, in addition to characterizing what DPI is, it is also important to understand what DPI is not. Box 3 highlights five common misperceptions about DPI.

The DPI Difference

Even though many systems now being built as DPIs—such as digital identity, payments, or data sharing—have existed for decades, some aspects of the DPI approach to digitalization for development are new. This includes: (1) a focus on creating shared building blocks, rather than digitalizing in silos, (2) the whole-of-society approach required to build and innovatively use DPIs, including the private sector, and (3) embedded functional and normative principles such as openness, interoperability, inclusion, transparency, strong governance, and data protection and privacy.

From Silos to Building Blocks

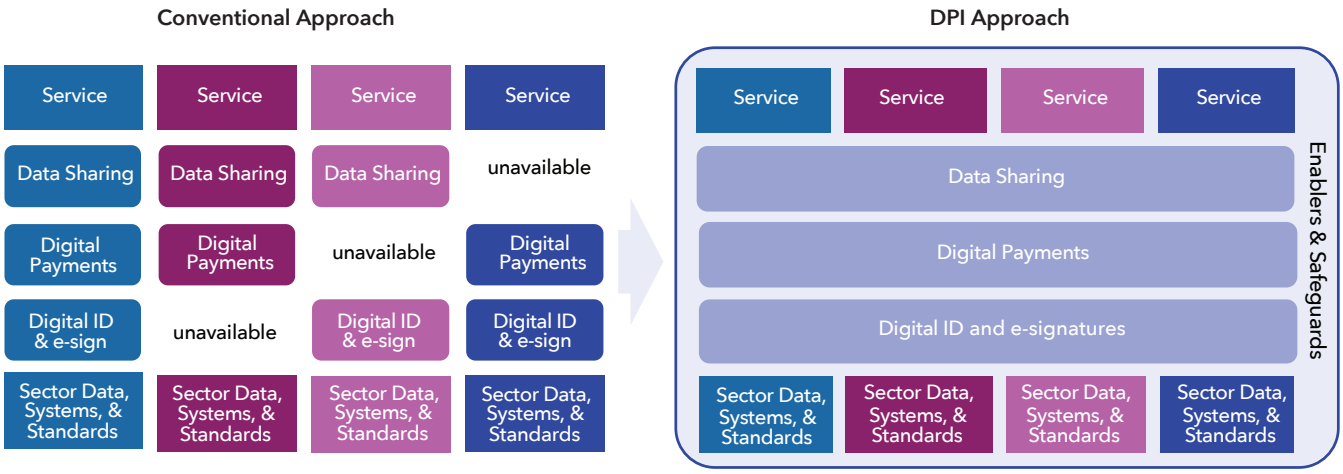
Under a fragmented approach to digitalization, each sector works to build its own end-to-end digital services. As shown in Figure 7, this begins with digitalizing sector data into digital registries and databases, developing management information systems (MIS), and then building the core functionality needed to deliver services online, such as developing in-house payment systems, functional IDs,[12] and single-sector data sharing platforms. In some cases, these services might attempt to leverage or integrate with digital systems in other sectors (for example, a social protection MIS cross-checking a health system to verify disability status), though often this is done through one-off connections and bilateral agreements.

While silo-ization may be logical from a service provider perspective, it means that each actor or sector is repeatedly reinventing the wheel for certain core functionalities, such as confirming that a beneficiary or customer is unique, requesting or making a digital payment, or verifying information about a person. In contrast, a DPI approach focuses on building a shared set of software or platforms that can be reused across sectors and plugged in—if needed—to their digital services. This saves time, cost, and human resources for sectors and allows them to focus on core competencies (such as developing electronic health records or implementing health-specific data and interoperability standards). In addition to these efficiency gains, DPI-specialized providers will typically be able to provide these services with higher levels of quality, security, and sustainability than entities without similar expertise. Building across silos is particularly important in an increasingly globalized world, as the digital economy flows across borders.

11 See Eichholtzer and Desai (2022).

12 Functional ID systems are created for a specific, limited purpose, such as social security number, tax IDs, or driver's licenses. While they may be recognized for other purposes, this often has limitations, and most countries have therefore implemented foundational ID systems (such as a national ID) as general-purpose proof of legal identity (see World Bank 2019).

Figure 7. DPI versus a conventional approach to digitalization



Source: Adapted from World Bank (2024).

A building blocks approach also enables multiple DPIs to be used together, with multiplier effects. For example, **India**'s DPI is a layered stack of multiple, interoperable digital building blocks created with the goal of enabling remote, paperless, and cashless service delivery across the country. It exists in the form of APIs—including for ID (Aadhaar), payments (Unified Payments Interface or UPI), brokered data sharing (Data Empowerment and Protection Architecture or DEPA), personal document storage and sharing (Digi-Locker), and e-signatures—made publicly available to developers, enabling them to improve upon and repurpose these APIs. Together, these APIs enable seamless service delivery, for example, by enabling remote workers to apply for social benefits, which are paid directly into their bank account, or electronically sign an application for a loan all on their phone (World Bank 2024a).

Whole-of-Society Approach

As the 2024 World Bank Digital Trends and Progress Report notes, "the paradigm shift" toward DPI can only be realized with a whole-of-society approach (World Bank 2024a). Breaking down silos and thinking about horizontal building blocks requires continuous coordination across government entities, including digital agencies, line ministries, and regulators; participation and collaboration of the private sector; and regular engagement with CSOs, the public, and other stakeholders. In **Uruguay**, for example, Desai et al. (2022) describe how each iteration of the Uruguay Digital Agenda—which includes a vision for data sharing and other DPI across the country—"has been a product of a multi-stakeholder process with representatives from government, academia, the private sector, and civil society organizations." They note that through the National Council for the Information Society, a diverse group of stakeholders continuously monitors the implementation of the Agenda, leading to high degrees of public trust. Similarly in **Singapore**, the government created a Smart Nation and Digital Government Group (SNDGG) as a government coordinating body to improve intragovernmental data sharing through a focus on developing and enforcing shared digital infrastructure, common standards (such as for data security), and interoperability of applications (Desai et al. 2022).

Focus on Outcomes and Principles

Finally, DPI recognizes that digitalization is about much more than technology. It represents a modern approach to digitalization that bakes in core principles around interoperability, minimization, inclusion, data protection, and more. This includes ensuring that DPI is technically designed and deployed in alignment with good practices and accompanied by sound legal frameworks, regulations, and institutions for accountable governance and oversight, data protection, and cybersecurity (G20 2023a). Furthermore, DPI advocates an outcomes-based orientation focused on inclusive adoption of digital services, private and public sector innovation, and the productive use of digitalization to achieve development goals.

2. DPI ECOSYSTEM

DPI does not exist in isolation; rather it is part of a broader ecosystem of technologies, systems, laws and regulations, capabilities, institutions, and frameworks required for the end-to-end deployment, adoption, and protection of digital services. Figure 8 provides a broad overview of this ecosystem, including (1) core DPI systems (including digital identity and e-signatures, payments, and data sharing), (2) non-technology enablers and safeguards, (3) technology enablers (such as energy, broadband, devices, data centers, cloud, AI, and big data), and (4) other digital systems and services across sectors (such as e-government service portals and applications, social registries, credit systems, and public financial management systems).

To succeed, economy-scale digitalization efforts must invest in each of these ecosystem components. As with the definition of DPI itself, this categorization may evolve over time with technology innovations and evolving standards and learning around DPI. However, it provides a useful starting point to disentangle some of the common questions around where the "bounds" of DPI start and end, and to identify complementary areas of investment needed to fully leverage and safeguard DPI.

The private sector plays a key role in the DPI ecosystem. While Figure 8 does not specify the roles of the public and private sectors, DPI can be owned, operated and managed by the public sector, the private sector, or a public-private partnership. More specifically, the private sector can be instrumental in the entire life cycle of the DPIs, from initial design and development to deployment, scaling and ongoing operation. Private investment is essential to the growth and success of DPI. For example, equity investments may be crucial for the development of innovative firms to support the development and uptake of high-impact use cases. In economies with limited private investment and an underdeveloped digital economy, adoption of DPI may not be as fast.

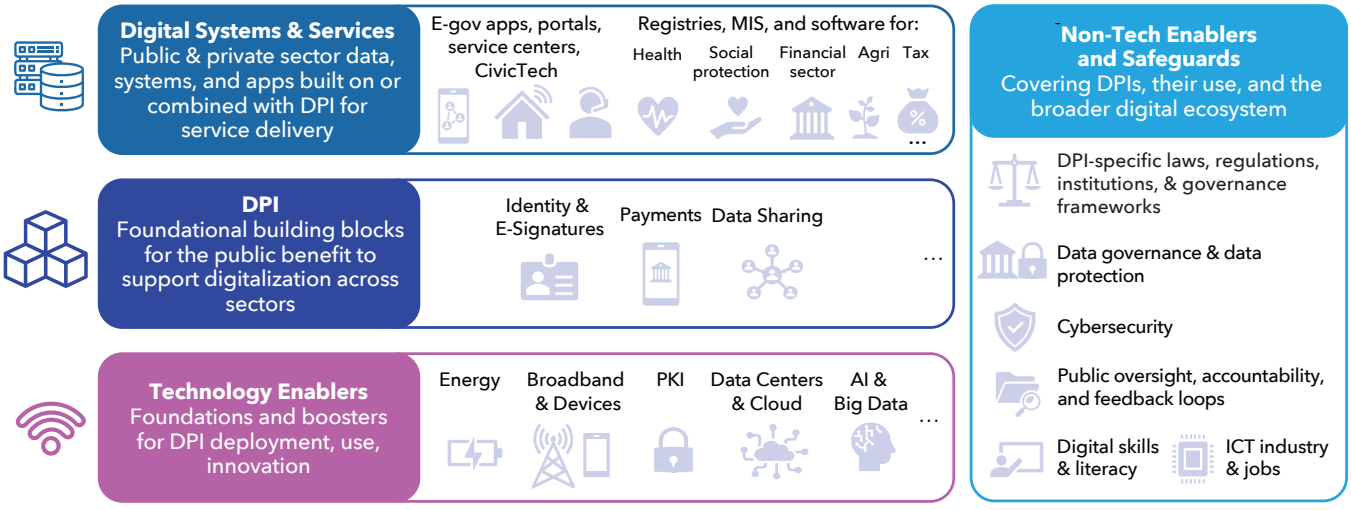
Core DPI Systems

DPI is a flexible concept, and therefore we should expect the emergence of new DPIs over time to enable digitalization at society scale. The World Bank Group will continue to document and provide guidance on new DPIs as they evolve; however, this paper focuses primarily on those systems—including digital identity and e-signatures, digital payments, and data sharing—that are well-accepted as providing "core" DPI functionality.

Digital Identity & Electronic Signatures

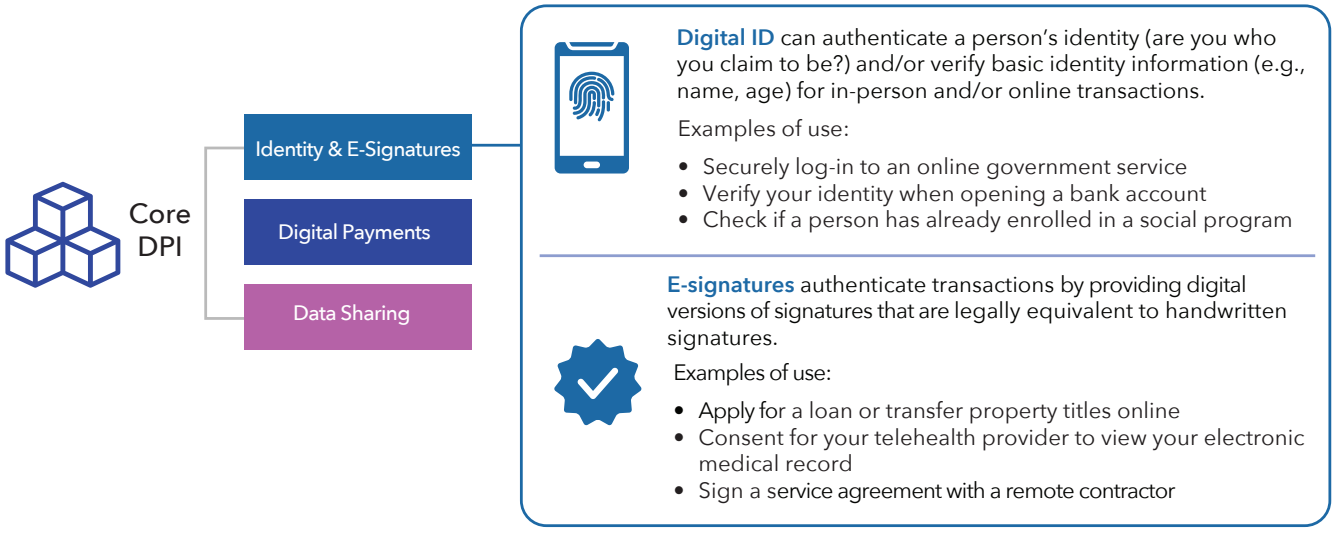
Identity and electronic signatures (e-signatures) are key ingredients in establishing online digital trust. While digital identity answers the question "with whom am I interacting?" e-signatures answer the questions "is this document or transaction (legally) valid?" and "did this person authorize this transaction?" Many transactions and interactions with government—whether in-person or online—require one or both types of questions to

Figure 8. Locating DPI within the digital ecosystem



Source: Original figure for this publication.

Figure 9. Role of digital identity and electronic signatures



Source: Original figure for this publication.

be answered. In some cases, such as securely logging in to an online account, digital ID alone may be sufficient. For other types of transactions—especially those involving a contract, agreement, or user consent—a legally valid signature may also be required after verifying the parties' identity. Digital ID and e-signatures thus complement each other in ensuring trust in online interactions. While it is possible to implement digital ID without e-signature functionality, there is a growing trend to implementing the two together, to take advantage of their complementary nature and similarity . For this reason, these are considered together in this paper.

Digital identity services enable secure and remote identity authentication and verification. These functions—confirming that the person[13] presenting an ID is the same person to whom it was issued (authentication) or verifying specific identity attributes or uniqueness (verification)—play a central role in many transactions online, as well as digitally enabled face-to-face services (World Bank 2022a). This includes online services that requires a secure login to prevent fraud and protect personal data, the ability of service providers to "know their customer," and the ability (when required) to link a person's online accounts to a person's legally recognized and unique identity (for example, to enroll in government benefits or vote online). Digital identity services can be facilitated through a wide variety of credential and authenticator technologies, including cards with chips or QR codes; PINs, passwords and one-time-passwords (OTPs); digital certificates; biometrics; and mobile applications and wallets, to name a few. These technologies—along with the degree of "identity proofing" when a person obtains a digital ID[14]—provide different levels of assurance or confidence in the identity a person presents.

The core functions of a digital identity DPI can be provided by a variety of ID systems. Most countries have some type of foundational ID system[15]—such as a national ID, population register, civil register, or similar—to provide government-recognized (also called "legal" or "official") forms of ID and documentation of vital events (birth, death, marriage, divorce) for individuals. As these systems have increasingly digitalized, many offer forms of legal ID, such digital national IDs or birth certificates, that can be digitally verified or authenticated for

13 Although this paper focuses on digital identity for individuals, DPI can also play an important role by providing trusted, and verifiable digital identity for other interacting parties, such as businesses, other legal entities, and devices. However, these are typically provided by separate systems (such as a business register), rather than a foundational (digital) ID system.

14 Digital IDs that provide higher levels of assurance often require in-person registration (or virtual, assisted registration) to "bind" the person to the digital ID—that is, to ensure that they are a real person and the person they claim to be. Linking this ID with a person's legal identity, for example, as evidenced through a birth certificate or national ID, also typically increases the level of assurance and is often required for digital identities used for government services. Ensuring the quality and inclusivity of national ID and civil registration systems is therefore of paramount importance to the trustworthiness of digital identity systems and the transactions they underpin.

15 According to data in Casher et al. (2024) 175 out of 198 countries with data have a foundational ID system, typically called a "national ID system" or similar.

in-person or online services.[16] As described in more detail in Section 3, the past decade has seen a rise in parallel digital ID systems that provide official online identity services either through a single provider (such as a digital agency), or through multiple public and private sector entities operated in a federation or decentralized architecture. As the demand for digital identity grows, new markets for private sector digital identity providers have emerged to add value on top of government-provided official ID. For the purposes of this paper, any of these systems can constitute a DPI if they meet the DPI criteria discussed above.[17]

E-signatures—which help ensure the security, authenticity, and integrity of digital transactions—are essential for digitalization. Analogous to written signatures in the physical world, e-signatures help establish confidence in the origin of digital data and documents and ensure that transactions carried out electronically are legally valid.[18] This is important for enabling remote signing of contracts or agreements, including documenting consent. E-signatures provide four core functions that facilitate online trust: (1) identifying the signer, (2) attributing the signature to the signer, (3) recording intent to sign, and (4) assuring the integrity of the signed data and protecting against tampering (Tullis et al. 2024). Implementing these functions requires a combination of dedicated legal frameworks, processes, and digital technologies. Some type of e-signatures, such as clicking an "I accept" box, provide low levels of assurance or security, while those based on digital signatures[19] technology using public key infrastructure (PKI) can provide the highest level of assurance, as shown in Box 4.

In many countries, digital identity has been a cornerstone or "first block" of a DPI stack. This relates to digital identity's role in helping to secure or enable digital payments and facilitate the safe exchange of personal data, and to the role that traditional ID and civil registration systems play in establishing legal identity to underpin rights and services.[20] In **Indonesia**, for example, the national ID card (e-KTP) serves as the basis for legal and digital identity, with new digital ID applications (including the IKD and INA Pas) built on top. In Uruguay, the ID **Uruguay** digital platform launched by AGESIC in 2019 has been a steppingstone for digitalization, enabling citizens to securely access over 190 digital services and complete more than 1,500 online procedures, including essential services like healthcare records, tax filings, and social security benefits (Public Digital 2023). In **India**, the Aadhaar Enabled Payment System (AePS), is a bank-led model enabling interoperable financial transactions at agents through biometric authentication. AePS supports basic banking services such as cash deposits, withdrawals, fund transfers, and balance inquiries, by using Aadhaar as the identity verification and authentication mechanism. In the **Maldives**, the eFaas platform provides a secure digital identity for accessing 128 digital service portals, spanning sectors such as public health, housing, local government, and finance. Building on this foundation, the government now aims to integrate eFaas with a secure data-sharing platform to enhance consent-based data sharing, reduce redundancy, and address data silos.

In some cases, e-signature capabilities are standalone systems, not implemented through an ID system. **Mexico**'s FIEL/e.firma (Advanced Electronic Signature) system, managed by the Mexican tax authority (SAT), has over 13 million users and has enabled the streamlining of administrative processes, improved tax compliance, and has enhanced the security and legal recognition of digital transactions across various sectors (Mifiel 2024). In **Indonesia**, e-signatures and a range of other trust services[21] are provided through licensed certificate authorities (PSrEs), which include both public entities and private companies.

16 For more details on the digital readiness of foundational ID systems globally, see Metz et al. (2024).

17 The forms of digital ID described in the paper include those linked to a person's official or legal identity, whether or not they are provided by the same entity that issues the foundational ID. Not included are those such as using Facebook, Amazon, or Google accounts to log-in to other websites or services on the internet via federation protocols.

18 Whether or not a particular technical implementation of an e-signature is legally valid depends on the relevant trust framework in the jurisdiction. Under **the European Union's** eIDAS, for example, only "qualified electronic signatures" (QES) that involve strong identity proofing and PKI are presumed legally valid. However, the role of an e-signature framework is to provide clarity and levels of assurance for various technical implementations (Tullis et al. 2024).

19 Note that the terms "electronic signatures" and "digital signatures" are not synonymous; the latter refers to one potential underlying technical implementation of e-signatures that uses digital certificates issued by certificate authorities (CAs) under a PKI. Digital signatures also have many broader uses such as secure internet communications. In addition to Figure 10, see Tullis et al. (2024 & 2025) for more on e-signatures and PKI.

20 For example, SDG 16.9 called on countries to provide "legal identity for all, including birth registration, by 2030." As countries have moved to digitalized their national ID and civil registration systems, providing these digital forms of identity can bolster the right to an ID in both the physical and digital worlds.

21 Electronic signatures are one of multiple "trust services" that provide confidence in digital transactions and could be built as DPIs given their central role in authenticating digital transactions. The UN Commission on International Trade Law (UNCITRAL) defines trust services as "an electronic service that provides assurance of certain qualities of a data message and includes the methods for creating and managing electronic signatures, electronic seals, electronic time stamps, website authentication, electronic archiving and electronic registered delivery services" (UNCITRAL 2023).

Box 4. Digital identity, e-signatures, and digital signatures

Digital identity, e-signatures, and digital signatures can be related but are not synonymous. This paper uses the following definitions:

- **Digital identity:** A set of electronically captured and stored attributes or credentials that uniquely identify a person and enable authentication of the individual and/or verification of identity attributes.
- **E-signature:** Analogous to written signatures, e-signatures help establish confidence in the origin of digital data and documents and ensure that transactions carried out electronically are valid. They are a legal concept that can be implemented through various technologies, from the very basic (signing your name on a touchpad) to the more advanced (for example, using digital signatures).
- **Digital signature:** A technical operation using public key cryptography, wherein a user's private key is used to digitally sign data, and their public key is used to verify the signature. Digital signatures are implemented using digital certificates provided by certificate authorities (CA) as part of a public key infrastructure (PKI). For more on PKI, see "Technology Enablers" later in this section.

To illustrate these complexities, here are some examples of how these functions overlap:

- IDs are often *digitally signed* by the issuing agency (using their digital certificate) to improve the integrity and security of the credentials.
- IDs are often used as *proof of identity* to link users to their e-signatures or digital signature certificates (for example, see Table 2).
- Digital signatures can be used to implement *high-assurance* digital ID authentication or e-signatures and some digital IDs include digital certificates to implement these signatures.

Source: Adapted from Tullis et al. (2024 & 2025).

Increasingly, however, e-signatures are built into the functionality of a digital ID. For example, **Argentina**'s national ID smartphone application, called Mi Argentina, includes a digital certificate to generate legally valid electronic signatures. Under **Sweden**'s BankID scheme, various banks issue credentials that include a PKI-based certificate for digital identity authentication. During authentication, this certificate creates an authentication token, which authorizes transactions under the eIDAS's "substantial" level of assurance. When an e-signature is required, the authentication token triggers the generation of a one-time digital signing certificate along with a signature at the "advanced" level of assurance (DIGG 2020). In addition, under the **European Union's** planned digital wallet (eIDAS 2.0), a high-trust electronic signature is integrated alongside a high-trust digital ID credential in one easily usable package that will be rolled out across the 27 EU member states by 2026 (Tullis et al. 2024).

Some high-risk or high-value transactions require a digital ID or e-signature that can provide a very high level of assurance or trust. This includes, for example, the use of PKI-based digital signatures that use strong cryptography and other processes .[22] Ideally, digital identity and e-signature ecosystems will provide multiple types of ID that enable user choice and various levels of assurance to facilitate a risk-based approach to identity verification across high- and low-risk transactions. Providing only high-assurance digital ID and e-signatures—for example, requiring biometric- and/

22 PKI is further discussed in "Technology Enablers," later in this section; however, it could also be considered as a separate DPI. For more on the distinction between digital identity, e-signatures, and digital signatures, see Box 4.

or PKI-based authentication for all interactions—can increase complexity and/or costs, and potentially exclude some users to the extent that they require owning or using more advanced devices or technologies. Similarly, providing only low levels of assurance is insufficient to move high-value or high-risk transactions fully online, such as voting, purchasing property, or issuing and signing contracts.

Countries can follow multiple models to build effective digital ID systems that serve as DPIs; however, notable gaps remain. According to World Bank estimates, there are still some 850 million people without *any* proof of their identity—paper based or digital—mostly concentrated in lower-income countries (Clark et al. 2022). Furthermore, an estimated 1.25 billion people do not have a digitally verifiably identity record or credential, while an estimated 3.3 billion people live in countries without a government-recognized digital identity for online transactions (Metz et al. 2024). And while a significant share of the population living in upper-middle and high-income countries do have a digital ID of some kind, many of these systems are not built with DPI functionality or norms in place. As such, they may not be interoperable or usable by diverse service providers, may not be widely accessible to the population, or may offer inadequate protections for personal data.

Similarly, there is room to make significant gains in e-signature capabilities globally. As of 2024, only 96 economies had fully operational e-signatures, of which 69 were high-income or upper middle-income countries. Some 35 additional economies with e-signature regulations have yet to develop technological infrastructure, reflecting that one of the core challenges to implementing trust services is the cost and complexity of developing sustainable business models for PKI as one of the core technologies underpinning high-assurance e-signatures (World Bank 2024a). At the time, progress had been made, including increasing moves toward cross-border interoperability of e-signatures to build the digital economy. For example, the **European Union**'s eIDAS regulation provides for cross-border interoperability across the EU, allowing for e-signatures created in one member state to be verified and legally recognized in any other. Interoperability is assured irrespective of whether the trust service was provided by a public- or private-sector entity (EU 2014 & 2024).

Digital Payments

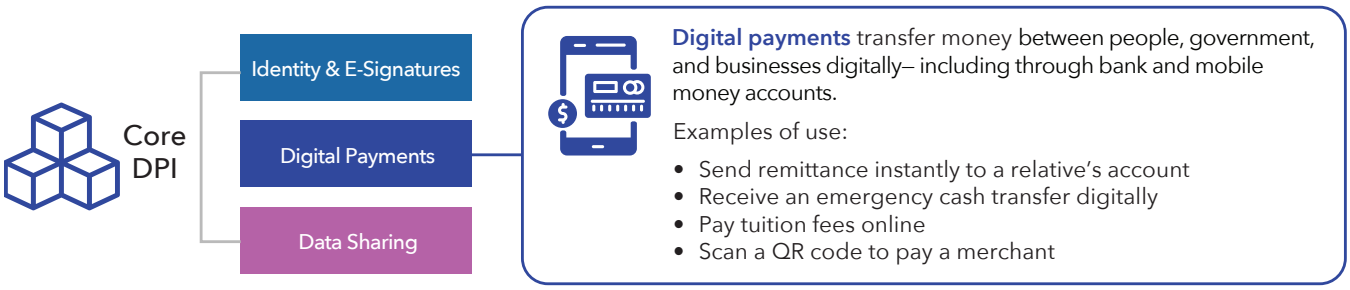
Digital payments enable more secure, convenient, interoperable, and cashless transactions. They allow individuals, businesses, and governments to transfer money easily and securely. This includes e-commerce and merchant payments, government-to-person (G2P) payments such as social assistance benefits; person-or-business-to-government (P2G or B2G) payments such as taxes; and person-to-person (P2P) payments among individuals. In addition to replacing the need to pay with physical cash or checks, digital payments enable users to receive payments remotely (for example, on their mobile phone via a bank or mobile money account), giving them choice about if, when, and where they want to cash out, save, or use the money digitally.

Technological innovation and changing priorities have led to a paradigm shift toward fast payment systems (FPSs). Traditional payment infrastructures in most jurisdictions consist of a real-time gross settlement (RTGS) system for large-value and time-critical payments, an automated clearing house (ACH) for low-value payments, card payment processing systems, e-money service providers (including interoperable infrastructure), and mechanisms for cross-border payments. However, the transition to an FPS allows for instant funds transfer and immediate fund availability to beneficiaries on a 24/7/365 basis. As an FPS evolves, it enables a diverse set of payment service providers (banks and non-banks) and supports a variety of payment instruments, use cases (domestic and cross-border), transaction channels, and overlay services. [23]

FPSs provides critical advantages, including offering immediate access to funds and lower fees, reducing switching costs, promoting interoperability, and encouraging the use of transaction accounts. This shift enhances platform competition and enables new providers to offer diverse services, thus increasing competition and dynamic efficiency within the payments ecosystem. Additionally, an FPS plays a crucial role in the digitization of government payments, enabling real-time revenue collection and efficient disbursement of time-sensitive payments. This infrastructure supports urgent transactions during emergencies, ensuring timely delivery of financial aid to vulnerable populations. The types of payment instruments supported by FPSs include credit transfers, direct debits, and e-money. Direct debits are available in

23 When comparing modern models for digital payments, it is important to clearly articulate how FPS differ from newer models, such as those promoted by Open Finance. A Payment Initiation Service Provider (PISP), as encountered in Open Finance frameworks, is not an infrastructure but a service model that allows third-party providers to initiate payments on behalf of customers directly from their transaction accounts, possibly leveraging an FPS for this purpose. While an FPS focuses on the underlying technology and network to facilitate instant transactions, a PISP leverages such infrastructure to enhance user convenience and broaden access to financial services.

Figure 10. Role of digital payments



Source: Original figure for this publication.

China, Hong Kong SAR, India, Nigeria, and Singapore, with development underway in Australia and Malaysia. E-money is supported in Chile, Hong Kong, India, Malaysia, Mexico, Nigeria, Thailand, and the United States. Credit transfers are universally supported across all jurisdictions that have implemented an FPS.

A growing number of countries have implemented an FPS as a core component of their DPI. Over the years, many countries have enhanced their DPI ecosystems through the implementation of FPSs. These systems unify a diverse range of providers and use cases, fostering interoperability and competition, reducing costs, and spurring financial inclusion and innovation. Approximately 70 emerging market and developing economy (EMDE) jurisdictions have launched these systems, with several more expected to go live in the near future.[24] Notable successes include Thailand, where PromptPay reached close to 20 billion transactions in 2023, Brazil, with 112 transactions per capita annually, and India, where 81 percent of all digital payments are processed through an FPS.[25] However, fewer than 20 EMDE countries have fully leveraged the complete range of functionalities that FPSs offer, such as merchant payments. Cross-border interoperability for payments has become a priority for many jurisdictions. For example, with the goal of adhering to EU standards and integrating into the Single Euro Payments Area (SEPA), the Western Balkans have adopted common legislation and payments infrastructure, modernizing the regional payment system to enable cost-efficient cross-border payments.

Data Sharing

Digital systems for sharing data can help optimize the flow and reuse of data in the digital economy, particularly across sectors. This includes protecting data that should not be shared, while simultaneously removing constraints that result in suboptimal data flows. For example, while much global attention has necessarily been paid to protecting personal data from exposure and misuse, it is equally important to enable easy sharing of data that could provide public benefit and enable better service delivery and digital innovation. Data sharing DPIs can enable entity-to-entity data sharing architecture (for example, a finance ministry agency sharing data with the tax authority), open data for public use (for example, open data portals and data lakes), and personal data sharing and management (for example, decentralized management of personal data and documents). As with other DPIs, data sharing software and platforms can be provided by the public or private sector; in particular, new markets for decentralized personal data and credential management applications like wallets are likely to grow substantially in the coming years.

The appropriate data sharing system depends on the purpose and type of data being shared. Systems that enable individuals, businesses, and governments to seamlessly and securely share or exchange data across (and within) sectors are key for many types of transactions, as well as for research and broader policy making. There are multiple technical solutions for data sharing depending on the type of data and other factors, including enterprise service busses, API gateways

24 Recent research from the Bank for International Settlements indicates that as fast payment volumes increased, the demand for small denomination banknotes decreased. This rise in fast payments also coincided with an increase in card payments, demonstrating that fast payments are a key driver in the digitalization of payment ecosystems. See Alberto Di Iorio et al. (2024).

25 See Bank of Thailand (2024), Alberto Di Iorio et al. (2024), and Reserve Bank of India (2024), respectively.

and exchanges, warehouses for open data, and verifiable credentials. These are discussed in more detail in Section 3.

One key parameter for data sharing architecture is whether the goal is to promote wide data reuse or to protect data from abuse. Data at risk of oversharing requires systems that enforce strict access controls and, in the case of personal data, gives control and transparency to people ("data subjects") over how their data is used. For example, **India**'s Data Empowerment and Protection Architecture (DEPA) creates a framework for third party "data fiduciaries" to facilitate consent-based data sharing on behalf of an individual, and with the legal obligation to act in their best interest. In contrast, systems designed to increase the reach of data, such as those aimed at increasing transparency and efficiency through open data, should be designed with accessibility, usability, and discoverability in mind. In the **Maldives**, where climate change poses significant risks, the government plans to develop a secure data-sharing platform integrated with existing DPIs to enable consent-based data sharing, remote service delivery, and improved sharing of non-personally identifiable data for climate adaptation.

Data sharing DPIs facilitate data sharing across sectors and should integrate into sectoral data systems. In addition to society-wide DPIs that enable data sharing and personal data management across sectors, some sectors will have their own specific data sharing protocols and platforms (such as for health data, which is highly sensitive) that can be built to interoperate with DPIs for cross-sector data exchange. As noted earlier, data sharing DPIs do not replace sector-specific data and interoperability standards—such as the Fast Healthcare Interoperability Resources (FHIR) standard in the health sector—but should be designed to interface with them.

As with other DPIs, trusted data sharing systems go beyond technology and are closely linked to laws, policies, and frameworks for data governance. In **Estonia**, for example, the X-tee platform—which enables data sharing for 1,700 services—is embedded in a robust data governance framework, along with technical controls such as a citizen portal to enable people to see how their data is used (World Bank 2022a). Furthermore, countries and regions are increasingly looking to implement cross-border data sharing to improve access to services, trade, and migration through multi-country frameworks such as **the European Union's** eIDAS and EU Digital Identity Framework (EUDIF). For instance, the Europass Digital Credentials for Learning project offers a trusted way to share verifiable diplomas and certificates, allowing easy verifiability by employers in any of the 27 EU member countries.

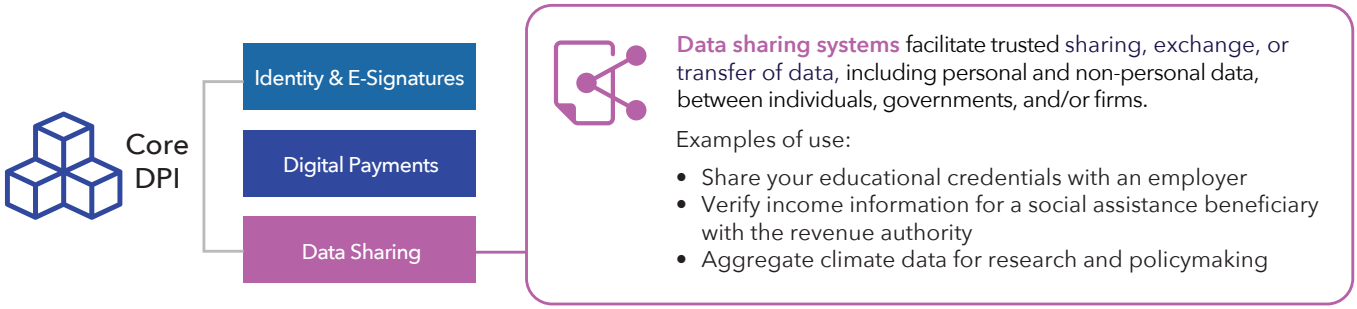
Non-Technology Enablers and Safeguards

DPI is much more than technology. This section outlines some of the key "non-tech" components of the digital ecosystem—sometimes referred to as "analog complements" (World Bank, 2016)—including legal frameworks, regulations, and governance requirements for DPI systems themselves, along with additional measures to ensure that DPI is safe, inclusive, and helps close rather than widen the digital divide.

Laws and Regulations

Each DPI requires appropriate enabling laws and regulations specific to the system. This includes legal and regulatory frameworks required to establish and operate each DPI with clear roles and responsibilities. Typically, this involves separate laws, regulations, or decrees related to each core DPI system, such as a national or digital ID law, laws on data sharing and access, laws on e-signatures, and laws governing digital payment ecosystems. In addition, it includes legal instruments required to enable the use of DPI for digital services and transactions and ensure legal equivalence with paper transactions, such as broad e-transactions and

Figure 11. Role of data sharing



Source: Original figure for this publication.

e-commerce laws and sector-specific laws (for example, as relevant for health, social protection, agriculture, and other sectors). Even if data sharing and e-signature capabilities exist, they will not reach their full potential if paper copies and handwritten signatures are still required by law.

Beyond those specific to DPI systems, broader legal and regulatory frameworks for data governance, and data protection are critical. Robust data governance practices, supported by tools that oversee the use and reuse of data throughout its lifecycle, are crucial for maximizing the value of DPI. Effective data governance must address both personal and non-personal data, recognizing their distinct characteristics and governance requirements. This is an important basis for all DPIs—including digital identity, payments, and data sharing—that engage in data processing.

Personal data requires stringent safeguards to ensure privacy and protection, which are fundamental for maintaining public trust in a DPI that processes this type of data. This includes the adoption of legal and regulatory frameworks for data protection alongside the integration of privacy-enhancing technologies within the technical design of DPIs. Core data protection principles include lawfulness, fairness, and transparency in data processing; purpose limitations to ensure data is collected for specific, legitimate purposes; minimization of data to collect only what is necessary; accuracy of data; storage limitations; integrity and confidentiality; and accountability. These principles are outlined in frameworks and instruments like the **European Union**'s General Data Protection Regulation ("EU GDPR"), the **Council of Europe**'s Convention for the Protection of Individuals with Regard to the Processing of Personal Data ("Convention 108+"), the **OECD** Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data 2013, and others.

Non-personal data, including aggregated, anonymized, or machine-generated data, also plays a pivotal role in driving innovation and informing decision-making processes through data sharing DPIs in particular. For non-personal data, the emphasis must be placed on ensuring data quality, accuracy, and accessibility, as these factors are critical for realizing the full potential of data-driven insights and innovations. However, the governance of non-personal data should be carefully calibrated to avoid unnecessary restrictions that could stifle innovation, which is central to the evolving role of DPI in various sectors. In addition, algorithmic bias must be prevented. Algorithmic bias can occur when the data or models used for analysis mirror or exacerbate existing biases, potentially resulting in unfair or discriminatory outcomes, such as denying credit to marginalized groups. Preventing algorithmic bias requires the use of diverse and representative datasets, regular audits to detect biased patterns, and explainability techniques to understand how algorithms make decisions.

Governance and Institutions

Beyond laws and regulations, each DPI system also requires broader governance frameworks, including policies and standards at the national and sector level (World Bank & IADB 2024). Most countries are unlikely to have a single framework on "DPI governance," as DPIs are typically provided by different entities—including the private sector—and governed separately. With digital identity systems, for example, these are often implemented by national ID, civil registration, or digital transformation agencies, with specific governance arrangements and institutions. Digital identity and e-signatures often also include "trust frameworks" that outline roles and responsibilities for ID and e-signature providers and users, requirements and specifications for specific levels of assurance (or trust) provided, and more.[26] For payments, governance frameworks encompass the structure, processes, and policies through which Financial Market Infrastructures' (FMI) decisions are made and decisions are managed, regardless of whether FMIs are publicly or privately operated entities.

Broader data governance also requires policies, standards, and guidelines to govern how data is processed, shared, and reused across the economy, including for DPIs. Data governance frameworks clarify the roles and responsibilities of various stakeholders, define mechanisms required for monitoring and enforcing compliance, and establish consistent definitions, formats, and protocols for effective exchange of data. Importantly, this broader framework will need to consider sector-specific data governance mechanisms especially as they relate to DPI use cases, ensuring alignment while accounting for the unique needs of individual sectors. This interplay helps maintain coherence across domains while enabling sectoral and DPI-specific policies to adapt to distinct regulatory, operational, and technological requirements.

Across and within DPIs, multi-stakeholder involvement in governance is critical. The success of DPIs requires buy-in across various sectors, institutions, and the broader public.

26 For detail on trust frameworks for federated ID ecosystems, see World Bank (2022b), for details on trust frameworks for e-signatures, see Tullis et al. (2024).

Involving a range of groups in the design and governance will improve accountability and contribute to the success of DPIs by ensuring that they meet the needs and concerns of diverse users (World Bank & IADB 2024). At a minimum, these groups should include government and private entities involved in building DPIs, service providers from across sectors who will use DPIs, regulators, and CSOs and community groups (such as in **Australia**, **Jordan**, and **South Africa**, as discussed in Section 3). Strong engagement in DPIs by CSOs helps strengthen their overall design andensure effective oversight and accountability of these systems in the long run.

Additionally, institutional capacity is necessary for the effective implementation and operation of DPIs. This involves clear lines of accountability and responsibility and allocating resources and training to ensure that frameworks are effectively operationalized, allowing countries to reap the benefits of DPI across the economy. For instance, **Korea** employs a three-tiered data governance structure. At the top, the Presidential Special Committee on Data Policy sets national directions and coordinates data-related projects between institutions. The Ministry of the Interior and Safety (MOIS) oversees public data initiatives, while the Ministry of Science and ICT (MSIT) oversees data produced and held by the private sector. Supporting both ministries, the National Information Society Agency (NIA) focusses on ensuring alignment between their efforts, exemplifying an integrated approach to data governance (Khoury et al. 2024).

Institutional capacity is particularly crucial for ensuring high availability and efficient responses to users' demands. Adequate resources, expertise, and organizational arrangements within implementing and operating entities are critical for managing the complexities of DPI development, including stakeholder coordination, technical design, and governance frameworks. High availability is a core requirement for DPIs; for instance, FPSs re expected to operate 24 hours a day, 365 days a year to provide uninterrupted access and reliability. Without sufficient institutional capacity, the risks of delays, inefficiencies, and misalignment with broader public policy objectives are significantly heightened. Strengthening internal capacity of operators and leveraging private sector expertise ensure that DPI initiatives are not only implemented effectively but also supported throughout their lifecycle to deliver long-term economic and social benefits. Moreover, aligning DPI development with broader strategies, such as national financial inclusion or government digitization initiatives, can optimize resource allocation and enhance institutional readiness.

Cybersecurity, Resilience and Operational Reliability

Operational risks, including cyber threats, are amplified in complex, interlinked systems like DPI. Operational risks in DPI arise from their heavy reliance on technological and operational components, making them vulnerable to disruptions, fraud, cybersecurity threats, and risks from connected third parties. Operational failures, such as IT disruptions, cyberattacks, or errors in processes, can severely impact the DPIs ability to provide essential services. Such disruptions may lead to significant economic losses, and reputational damage. For example, in the financial sector, in extreme cases, operational failures may lead to systemic risk by undermining confidence in the financial system.

For this reason, policy guidance and robust frameworks for mitigating operational risks and for cyber resilience in the financial sector already exist, with implications for broader DPI. For example, the GPFI provides a policy framework to ensure the secure and resilient development and governance of DPI (Alber et al. 2023). More broadly, the Principles for Financial Market Infrastructures (PFMIs) also provide a robust framework to mitigate operational risks across Financial Market Infrastructures (FMIs) including Fast Payments Systems (FPS) (CPMI and IOSCO 2012). The recommendations across these frameworks advocate for the development of DPIs incorporating privacy-enhancing technologies, robust security measures, resilience against attacks or system failures, and sound risk management to build trust. They emphasize continuity planning to ensure uninterrupted operations and encourage adaptive, risk-based regulatory, supervisory and oversight frameworks tailored to the evolving risks posed by DPIs and new entrants. Additionally, they highlight the need for transparent governance stakeholder representation to safeguard public interest. Equally important is the development of features within DPIs to enhance customer protection, reduce risks, and foster trust. By leveraging these frameworks, countries can assess their financial infrastructure risks and work toward minimizing them.

The rapid adoption of Fast Payment Systems (FPS) introduces heightened cyber risks, such as ransomware and DDoS attacks, posing systemic threats to financial stability.[27] Effective risk management is needed to ensure seamless operations even under cyber threats, reducing disruptions that could compromise the overall functioning of the economy. To address these risks, tailored guidance and leading practices have been developed for FPS ecosystem participants, including payment system infrastructure operators, payment service providers, and end users.[28] This guidance emphasizes comprehensive cybersecurity programs across people, processes, and technology layers, leveraging internationally recognized frameworks and standards. A risk-based approach is recommended to prioritize resources for critical threats, with tailored risk management frameworks. Continuous monitoring, regular testing of cybersecurity controls, and proactive measures like encryption, secure access channels, and identity management can contribute to operational resilience. Collaboration through information sharing and cybersecurity awareness programs is also essential for robust defense against evolving cyber risks.

Ensuring the protection of both personal and non-personal data in practice also requires strong cybersecurity measures. This includes cybersecurity strategies and legislation, institutions and capacity building for cybersecurity incident response, and public awareness and training to improve cybersecurity skills within government, businesses, and the general public. For example, both **Singapore**'s "Digital Readiness Blueprint" initiative and Uruguay's central coordinating body for digitalization (the *Agencia de Gobierno Electrónico y Sociedad de la Información*, or AGESIC) have sought to prioritize cybersecurity capacity building and related digital skills (Desai et al. 2022) as a key component of their strategies, which contributes to the reliability of their DPI.

Continuity strategies to avoid disruption in the provision of DPI services is also crucial. The goal of DPI is to provide building blocks for the delivery of digital services across sectors—the reliability of these systems is therefore paramount to building trust, avoiding service disruptions, and managing reputational risk. This requires backup systems and disaster recovery sites, but also a deep analysis of potential failure scenarios, their probability, and impact. This is particularly important in cases where a specific DPI represents a single point of failure and requires technological and operational continuity strategies and established protocols that allow for timely communication and resolution of service interruptions.

Digital Inclusion, Literacy, and Skills

"Inclusion first" is a core principle of DPI. As with data protection, this requires a multi-pronged approach, including the technical design of a DPI (such as complying with design principles around universal accessibility) and legal and regulatory frameworks to ensure non-discrimination in DPI access and use. For example, as services increasingly move online, it is important to ensure that people with challenges using digital technology are not left behind due to difficulties accessing these services or prior exclusion from systems (such as IDs) that may be prerequisites for access. While DPIs can facilitate better access to services for many people, digital delivery should not be the only option for people to receive basic services or exercise their rights. Paper-based or assisted options, along with clear exception handling mechanisms when digital technologies fail, are essential. For example, **Cambodia**'s Verify.gov.kh document verification platform includes the ability for users to print documents that can be digitally verified using QR codes.

Proactive measures are needed to ensure that the potential benefits of DPIs reach everyone. The digital divide is a market failure; closing it requires systematically identifying and addressing barriers to digital adoption and use. This includes dedicated efforts or campaigns to reduce existing gaps in connectivity (such as broadband and devices) and DPI access (such as lack of foundational IDs or financial accounts needed to get the most out of digital identity and digital payments) and promote uptake of DPI-enabled services among groups most likely to be excluded. In **Mozambique**'s conflict-affected Cabo Delgado province, "one-stop-shop" mobile registration brigades, offering civil registration and national ID registration services, were set up to (re)register and provide official identity documents to internally displaced persons. These mobile brigades use simplified registration procedures and charge no fees to enable same-day registration and credential issuance for the most vulnerable, and enabled more than 75,000 people to obtain official identity documents and use these to access services, education, and job opportunities (World Bank 2023).

27 The World Bank's Project FASTT addresses the growing cyber risks associated with the adoption of FPS by providing tailored guidance and leading practices to safeguard the FPS ecosystem. For guidance on cybersecurity please see (World Bank 2025).

28 More broadly, financial sector standard-setters have underscored the critical role of FMIs in ensuring financial stability and economic growth by maintaining robust cyber resilience. See CPMI and IOSCO (2016) which supplement the PFMI and offer detailed recommendations on addressing escalating cyber threats.

Such efforts also require—and can be opportunities to provide—basic digital literacy training and education. Even if people have access to DPI and DPI-enabled services (for example, through an application on their mobile phone), they may need additional training and education to understand, trust, and use these services. In **Ukraine**, the Diia. Education online platform offers free digital literacy courses, including a national digital literacy test (Digigram) aligned with the European framework of digital competencies. The initiative extends beyond online resources, supporting over 6,000 offline hubs to reach citizens across the country, bridging gaps in digital skills and access (Ingram & Vora 2024). In **Bangladesh**, the BRAC Shakti program[29] was established in 2020 to boost confidence among women in using digital financial services. It employed a gamified approach to surround women with the peer support they need to explore, learn, and build comfort using new digital tools. Women are introduced to the program through their peers and are then onboarded to a small group where they learn about savings using mobile money and navigating other household dynamics around finances. Every two weeks, women go with the group to cash in their money at a mobile agent. As they deposit money, they earn rewards such as cash-back bonuses, among others. This gamified, peer-based learning approach was instrumental in reducing women's reliance on other household members, thus building their trust and confidence when making or receiving payments digitally.

Technology Enablers

DPI does not exist in a vacuum. The ability to deploy and use DPI relies on strong technology foundations, including connectivity, devices, PKI, data hosting, and cloud computing, and can also leverage advances in data-driven innovation, such as artificial intelligence (AI). DPI can also contribute to the development of new technologies including AI by improving data sharing and creating new markets for DPI-related AI applications.

Connectivity and Devices

Broadband connectivity and access to devices are crucial foundations for DPI and any digitally enabled service. While some DPI applications can be used without the internet—for example, scanning a QR code printed on an ID as a low-assurance form of identity verification—they still overwhelmingly rely on physical infrastructure for digital connectivity and individual access to devices. In rural and low-income regions that remain underserved by high-speed internet, or where access to smartphones (or even feature phones) is low, the opportunities for end-to-end digital service delivery will remain lower. As part of their efforts to expand internet access, many countries are investing not only in hard infrastructure, but also in "hybrid" service points where people can physically come to access online services. For example, **Bangladesh** has built over 9,000 "Digital Centers" run by young entrepreneurs that provide last-mile connectivity and access to over 300 government services to help "bridge the gap" between physical and digital services (Chowdhury 2024).

Public Key Infrastructure (PKI)

PKI—a combination of cryptographic technologies with complementary policy, organizational, and process elements—is an essential ingredient for online trust.[30] Under a PKI, Certificate Authorities (CAs) issue digital certificates to users (e.g., people, firms, government entities) that allow them to digitally sign documents and encrypt or authenticate information. At a basic level, these digital signatures and certificates enable secure web browsing by helping to establish secure communication channels (such as via the transport layer security or TLS protocol). PKI is also required for implementing high-trust digital ID and e-signatures, as discussed earlier in this section, and for securing digital payments and data sharing. Although the term "PKI" implies a single, unified infrastructure, there are often multiple PKIs operational in a given jurisdiction, including those provided by the public and private sector.

In the financial sector, for example, PKI supports the end-to-end encryption of payments data and the use of tokens to replace account details for enhanced security. PKI also supports robust authentication and transaction signing from financial transaction participants and operators at a system level. For example, FPS operators require participants to authenticate using digital certificates, such as x.509. Furthermore, each participant is required to digitally sign payment messages using the certificate issued by a trusted authority (in some cases the operator of the FPS). Data sharing applications similarly rely on PKI for secure transmission of data and authentication between data senders and recipients. For more on PKI, read Tullis et al. (2025).

29 For more, see https://www.ideo.org/project/brac-shakti.

30 For this reason, PKI could also be classified as a DPI, as it provides essential, society-wide functionality, and can be built with DPI specifications and principles. For the purposes of this paper, however, it is classified as an underlying technology.

Data Centers and Cloud

Modern data hosting and computing solutions are required to support DPI growth and expansion in a scalable and secure manner. Implementing DPI systems and platforms requires access to highly secure, reliable, and accessible data hosting environments to ensure trust in and availability of DPI. These hosting environments, whether on premises or accessed through the cloud, must conform to high security standards while ensuring that DPI-based services meet performance and accessible requirements.

To enable real-time processing, storage, and exchange of large volumes of data, operators of DPI platforms increasingly leverage the cloud in DPI deployment. DPI operators may make DPI services available to users over the cloud, deploy the DPI platforms themselves in cloud environments, or a combination of both. While some DPI operators use private cloud solutions or host DPI platforms in their own data centers, others leverage public cloud services to help promote scalability, reduce costs, improve performance, ensure security, and give the flexibility to meet the evolving data storage and processing needs of DPI ecosystems.[31] These approaches can reduce some risks of vendor lock-in for DPI operations, as well as enable innovation through cloud-based DPI services.[32]

Data-Driven Innovation

New technologies have the potential to boost DPI development and applications, including advances in artificial intelligence (AI), machine learning (ML), quantum computing, edge computing, and more. For example, AI and ML were pivotal in augmenting DPI during **India**'s massive COVID-19 vaccination drive. The CoWIN platform, built using an open-source platform DIVOC (Digital Infrastructure for Verifiable Open Credentialing),[33] used AI algorithms to optimize vaccine distribution, appointment scheduling, and real-time monitoring (Kumar & Veer 2021). AI helped predict demand patterns and ensure equitable vaccine allocation across different regions. Edge computing also has the potential to extend DPI-based digital services. In **Brazil**, for example, processing data locally at edge devices enabled healthcare providers to offer real-time diagnostics and telemedicine even in regions with limited connectivity, thus extending services to underserved populations (Silva et al. 2022).

A DPI approach can also be used to strengthen the development of new technologies. **Korea**, for example, has built a public infrastructure for data sharing and processing with the goal of supporting AI innovation (Khoury et al. 2024). Another example is in the **European Union**, where projects like the European Open Science Cloud and various AI research initiatives including the AI4EU platform[34]—which leverages DPI for data sharing and digital identity—connects AI researchers, developers, and users across Europe providing a virtual platform for collaboration.

Broader Digital Systems and Services

DPI does not deliver services in a vacuum—it works with and for a host of digital systems across sectors. Although DPIs such as digital identity and digital payments represent standalone digital services themselves, the power of DPI is its ability to integrate into a variety of sector applications. For this to succeed, sectors must have a variety of digital systems, including digitized databases and registers, interoperable information systems, and sector-specific data standards and digital-ready laws and regulations. A relentless problem-driven, user-centric focus, rather than an over-emphasis on technology, is required for effective DPI adoption. Strategic investment in the tools, practices, and institutional conditions required to provide good services is essential for scalability. Examples of these systems across different sectors are presented in Figure 12.

DPI can help strengthen myriad sector-specific applications, information systems, and registries to improve digital services and transactions. For example, rolling out digital registration and direct deposit for a social assistance program may use a dynamic social register with data on potential beneficiaries, management information systems (MIS) to determine eligibility, and applications for online registration. A digital identity DPI can help improve the integrity of the social register (by ensuring that each person registers only one time), accurately map unique beneficiaries to their accounts, and facilitate online registration (verifying the identity of a new applicant). A data sharing DPI can help verify eligibility by cross-checking applicants' income levels against the tax system, while a digital payment DPI facilitates instant payments to beneficiary accounts.

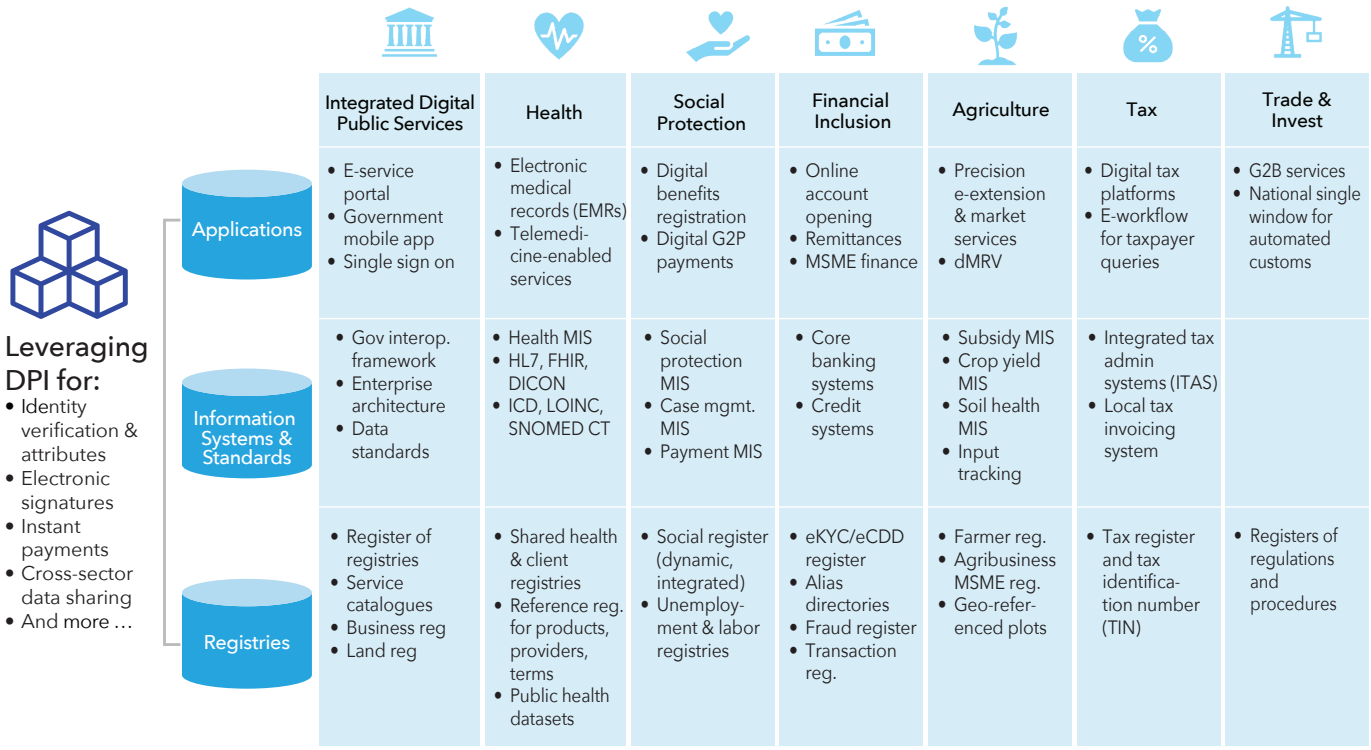
31 For example, over-reliance on public sector investment in cloud infrastructure or regulatory uncertainty can deter private investments in cloud needed to boost the digital economy and ICT industry. For more on cloud, see Gelvanovska-Garcia et al. (2024).

32 See Varma et al (2024).

33 For more, see https://divoc.digit.org/.

34 For more, see https://www.ai4europe.eu/about-ai4eu.

Figure 12. Example digital systems by sector



Source: Original figure for this publication.

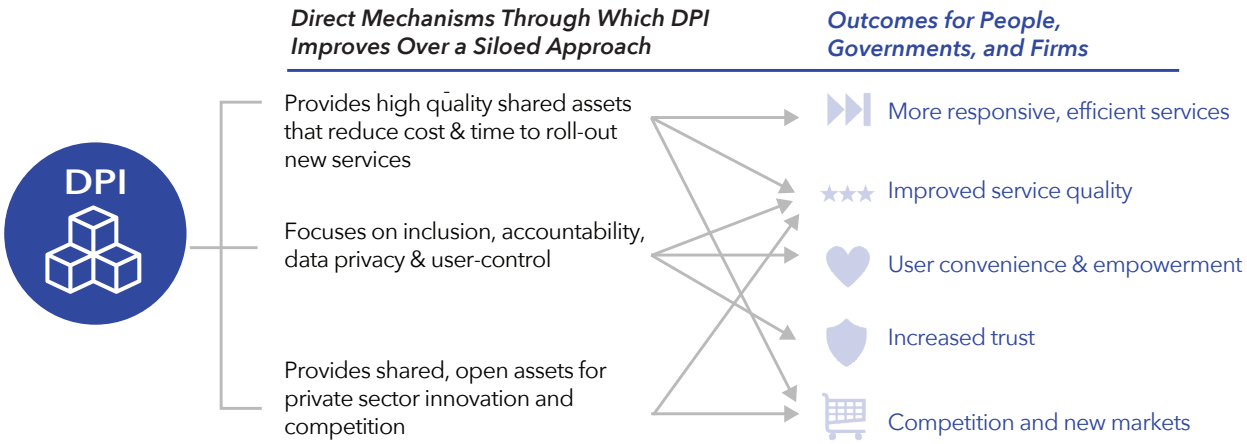
Integrated digital public service (DPS) layers and access points are often closely linked to DPI. DPS can include whole-of-government enterprise architecture, interoperability frameworks, single-sign on (SSO) e-service portals, and government mobile apps designed to provide integrated delivery of digital government-to-person (G2P) and government-to-business (G2B) services. Countries such as **Ukraine**, **Brazil** and **Jordan** have integrated DPI directly into this "one-stop-shop" approach to digital government. In **Jordan**, for example, the Sanad application and e-services platform includes digital ID and e-signatures functionalities that enable citizens to access over 2,000 services, including applying for government benefits, accessing personal records, digitally signing documents, and making bill payments.

Like DPI, DPS service layers and applications are sector-agnostic, and provide soft infrastructure and shared tools to architect a seamless, user-centric service delivery experience across all government agencies and providers. They also improve government efficiency by minimizing duplicative and conflicting digitalization initiatives across ministries. The core difference is that while DPI can be built, owned, and operated by the public and/or private sector, DPS systems are generally publicly owned and operated and typically only facilitate access to government services. Furthermore, DPS technologies are often bundled with broader change management and institutionalization of digital government reforms designed to enable a "whole-of-government" approach to digitalization (versus the DPI focus on "whole-of-economy" or society).

3. DPI AND DEVELOPMENT

A DPI approach to digitalization has many possible benefits, but also some obstacles. This section provides a concise theory of change for DPI and where we might expect it to have important impacts for development, followed by a summary of potential challenges and risks.

Figure 13. Potential impact: DPI versus a siloed approach



Source: Original figure for this publication.

Benefits of DPI

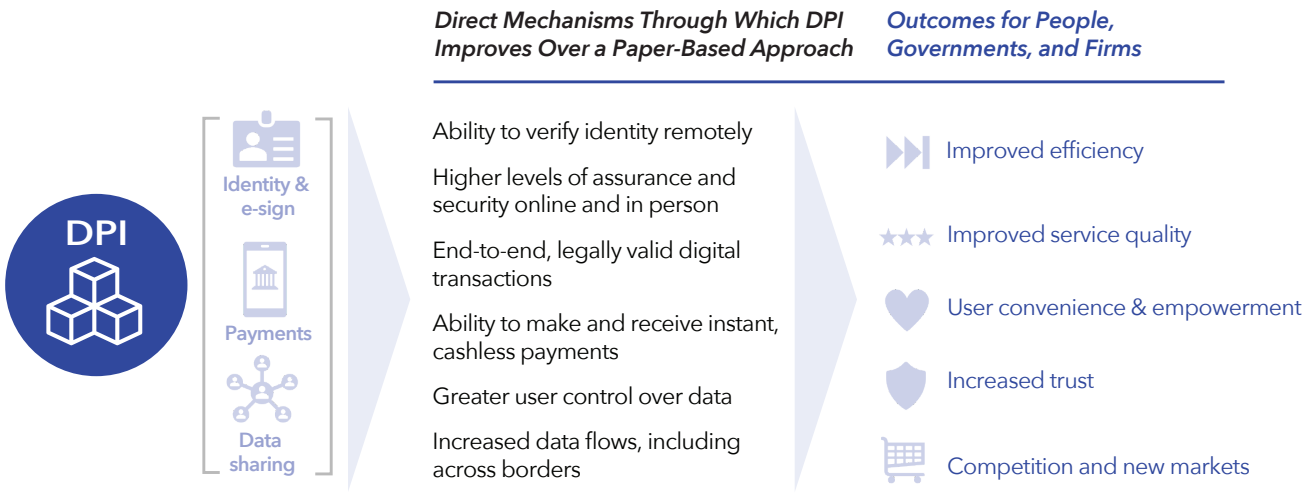
DPI has the potential to positively impact multiple development outcomes through both direct and indirect pathways. Figure 13 highlights three direct mechanisms for impact based on how the DPI approach of providing "foundational digital building blocks for the public benefit" is expected to improve outcomes, compared to following a traditional "siloed" approach to digitalization:

1. The availability of high-quality shared digital building blocks can significantly improve efficiency and reduce costs of government and private sector service providers, accelerating the development of new services.
2. By providing systems that focus on inclusion, public accountability, data privacy and protection, and user control, DPI's public benefits orientation can improve consumer experiences and empowerment, the quality of services and data, and online trust and security.
3. Providing open, shared building blocks can enable significant private sector innovation and competition, potentially further improving service quality and efficiency, and helping to develop new services, developer communities, and digital markets.

For example, DPIs can transform competition across markets by lowering entry barriers, enabling smaller players to challenge established firms, and fostering innovation. By democratizing access to data, automating processes, and promoting interoperability, DPIs reduce transaction costs and address information asymmetries, creating a more dynamic and inclusive marketplace. Innovations like digital ID systems, data-sharing platforms, and payment systems enhance accessibility, empowering new entrants and improving consumer choice through better services and personalized offerings. In **Brazil**, the introduction of Pix, a real-time payment system, has increased competition by enabling small banks to offer comparable services to larger institutions, attracting more deposits and narrowing the deposit rate gap while enhancing depositor benefits (Sarkisyan 2024). However, while open standards and equitable access are critical for market inclusivity, robust regulatory oversight is essential to ensure fairness, prevent market dominance, and safeguard against risks like data breaches and cybersecurity threats.

The case of digitalizing G2P payments illustrates these benefits. As summarized in the World Bank Digital Progress and Trends report (World Bank 2024a), for example, digitalizing G2P payments has contributed to 865 million people worldwide opening their first financial institution account to receive money from the government (Demirgüç-Kunt et al. 2022), and provided benefits such as reduced waiting times for payments (**India**), greater control of financial resources by women (**Pakistan**, **Niger**, **India**), and reduced time required to complete services (**Singapore**, **Estonia**). Digitalizing G2P payments has increased competition among payment service providers (**Zambia**) and lowered the cost of onboarding clients (**India**, **Singapore**) (World Bank 2024a). For governments, it has also reduced the cost of payments delivery (**Zambia**), reduced leakages (**India**), and enabled the rapid scaling of emergency benefits (**globally** during the COVID-19 response) (World Bank 2024a). To the extent that DPI enables faster, more efficient, and more secure scaling of digital services like G2P payments, its potential indirect impacts on development are sizable.

Figure 14. Potential impact: Core DPIs versus paper-based systems



Source: Original figure for this publication.

In addition to the overall benefits of a DPI approach, specific DPI systems provide direct benefits compared with non-digital systems. These mechanisms of impact are detailed in Figure 14, and articulate the ways that specific DPIs can improve efficiency, service quality, user convenience and empowerment, digital trust, and market innovation. There are numerous examples of these impacts around the globe. In **Singapore**, eKYC—facilitated by the Singpass consented data-sharing service—reduced the time to complete digital transactions by 80 percent (OECD 2022). In **Estonia**, the government, citizens, and residents save 820 years of working time every year thanks to the X-Tee data-sharing platform (Vainsalu 2017). In **India**, the Aadhaar ID system has reduced the onboarding cost for firms from approximately US$23 to less than US$0.15 (World Bank 2018).

To the extent that DPI accelerates digitalization, it can improve downstream outcomes for people, governments, and businesses. As noted above, DPI enables governments and businesses to develop faster and better services that would not have existed otherwise. For example, enabling governments to quickly roll out a social assistance program following a crisis, empowering individuals to open accounts or use their transaction history to access credit, or allowing patients to swiftly access telehealth services with full access to their health history. These faster and better services are improving healthcare, climate resilience and financial inclusion, among other positive outcomes, partially enabled by DPI.

Challenges and Risks

While DPI holds potential for transforming service delivery and fostering economic growth, its implementation still faces significant challenges. One key obstacle is existing gaps in availability and access to DPI systems and their precursors both across and within countries. As noted above, for example, an estimated 850 million people lack official identification—around half of whom are children whose births have not been registered—and 3.3 billion lack digital identities that can be used for online services (Metz et al. 2022). Similarly, some 1.4 billion adults lack accounts to safely store money and make daily transactions via digital payments (Demirgüç-Kunt 2022). Furthermore, the quality and accessibility of data are crucial for effective DPI, yet many countries are struggling with data silos, poor data management practices, and limited digitalization of government services. Procurement practices, technology choices, thoughtful policy and regulatory frameworks, and government capacity play a crucial role in DPI success. Unsustainable technology choices, vendor lock-in, and inadequate government capacity to design, implement, and maintain DPI systems can hinder progress.

The implementation and adoption of DPI can encounter political and change management challenges to the extent that it disrupts existing power structures, governance models, and vested interests. Shifting from traditional siloed models of digitalization to a DPI approach requires overcoming institutional inertia, as established processes, norms, and bureaucratic practices may resist change. Governments may face

difficulties in phasing out legacy systems, which have become deeply embedded in workflows and are often supported by long-term contracts with service providers. This inertia can be compounded by a lack of political will, especially if reforms threaten entrenched interests or alter the distribution of power across government agencies and with private stakeholders. Managing these dynamics requires strong leadership, multi-stakeholder engagement, and transparent policymaking to ensure that DPI initiatives serve the public interest. The transition also requires significant investments in change management, as public officials and end-users must shift to new ways of working and interacting with digital systems. Developing clear roadmaps, incentivizing adoption, and providing continuous capacity-building are critical to overcoming these barriers. Digital citizen engagement approaches can also help address resistance to change from end-users.

The persistence of temporary or stopgap solutions could also hinder DPI development in the longer term. In some cases—such as during COVID response and vaccination campaigns— governments need immediate solutions to deliver a specific service and cannot wait for DPI or interoperability frameworks to be developed. While one-off digital systems can meet an urgent short-term need, they can create challenges down the line, such as a proliferation of data silos, inconsistent standards, and duplication of efforts. Overreliance on quick fixes can undermine the long-term sustainability of digital systems and the ability to adopt a DPI approach in the future, locking governments into costly systems that are difficult to upgrade or integrate. To avoid these pitfalls, governments can adopt a strategic approach to DPI development, emphasizing interoperability, scalability, and alignment with broader national goals, and building DPI systems in parallel with urgent sector projects. This requires building institutional capacity not only for immediate implementation but also for continuous improvement and system upgrades as technologies evolve.

Digital inclusion and data privacy and protection are critical concerns for any digital system, particularly those that deal with personal or sensitive data. While DPI can help bridge the digital divide by improving the availability and accessibility of services, its success hinges on ensuring equitable access to DPI systems, digital literacy, and affordable internet connectivity and devices. The collection, storage, and sharing of personal data for DPI systems—including digital identity, personal data sharing, and payments information—also raises potential concerns about privacy violations, data theft, misuse, and surveillance. While the goal of a DPI approach is to mitigate many of these risks by embedding a public benefit orientation that prioritizes inclusivity, data protection, user control, and oversight into the design of DPIs, broader safeguards are needed (UNOSET & UNDP 2024). This includes adopting robust legal and policy frameworks for data protection and privacy, cybersecurity, and non-discrimination, building strong oversight bodies and public engagement, outreach to marginalized and vulnerable groups, and more. Critically, these safeguards should not only be limited to DPIs themselves, but to how they are used and integrated across sectors.

Finally, low levels of online trust and digital skills present significant barriers to DPI adoption. Reluctance to trust digital services can impede widespread use. New users of digital technologies often have lower digital skills and thus can be at greater risk of predatory practices. Addressing these challenges requires building trust through transparent governance, robust security measures, capacity building and effective communication. For example, public engagement strategies can constitute a proactive approach to risk mitigation. By engaging users early and often, providers can identify potential issues before they become widespread problems, such as conducting public consultations on data sharing policies to address privacy concerns and build trust in DPI systems from the outset. Similarly, not all countries and service providers interested in adopting DPI have the necessary internal skills or capacity for development or oversight that ensures robust security measures. Investing in digital skills development programs for both individuals and government officials is essential to ensure a digitally literate population capable of navigating and benefiting from DPI initiatives. Evidence assessing the risks and potential mitigating solution to DPI-enabled services is nascent and should be expanded.

Box 5. DPI in the context of fragility, conflict, and violence

Digital Public Infrastructure (DPI) holds transformational potential for countries affected by fragility, conflict, and violence (FCV) but also presents unique and more pronounced obstacles. While many of the challenges and opportunities outlined in this report also apply to FCV-affected countries, the journey to develop and adopt DPI in an FCV setting will be markedly different and will require attention to systemic challenges.

FCV countries face fundamental challenges require adaptive and innovative solutions:

- Risks related to the misuse or mismanagement of personal data can be heightened due to weak institutional or legal capacity, potential compromises to critical infrastructure (such as data centers) that can result in data loss or exposure, and potential incentives for surveillance or persecution leveraging data. Ensuring robust data protection and privacy is critical to prevent such misuse.
- Mistrust in government and lack of legitimacy can lead to low public demand for digital public services. People may prefer informal access to services, undermining the adoption of DPI. Political dynamics in FCV countries often include economic and institutional capture and systemic corruption, which can obstruct or distort DPI development and use. Capacity constraints are another major challenge. Conflict and disaster-related destruction can severely impact institutional and infrastructure capacities. The loss of human resources, fragmented international assistance, and lack of fundamental enablers further exacerbate these constraints.

  In post-crisis contexts, there is often an urgent need for sector-specific quick wins. Balancing these immediate needs with a holistic DPI approach can be challenging but is essential for sustainable development.

Despite these challenges, the transformational potential of DPI in FCV contexts is significant:

- Experience has shown that digital technologies can facilitate the rapid resumption of services following conflict or disaster-related disruptions. In **Haiti**, for example, mobile money has been instrumental in delivering social assistance payments in the Grande Anse area where distribution of cash would be otherwise challenging.
- While the initial investment in applying a more holistic DPI approach in these contexts is more time and resource intensive than parallel sectoral system development, upfront investments in DPI (and its associated enablers and prerequisites) could generate an important multiplier effect and better returns on investment over the medium term. In **Mozambique**, a combined birth registration and ID registration exercise for internally displaced persons across the conflict-ridden province of Cabo Delgado improved access to services and assistance.
- DPI can serve as a critical enabler for restarting economic activity and jobs—and importantly—breaking monopolistic and predatory wartime and post-disaster economic drivers. In **Ukraine**, for example, the Diia app and ecosystem which leverage DPI were critical to provide a single access point for nearly 120 public services, facilitating seamless service delivery for Ukrainians regardless of their location. Digitalization of services including DPI can also improve recovery trajectories by providing more efficient pathways for institutional and service capacity that do not require the traditional "brick and mortar" approaches to reconstruction and re-establishment of services.
- Last but not least, the principles of inclusion, user-centricity, and participation that underpin the DPI approach can yield a powerful peacebuilding impact in a post-crisis context, serving as a vector for more equitable governance and service delivery and the rebuilding of the social contract between individuals and the state.

Implementing DPI in FCV contexts is undoubtedly more challenging than in higher and middle-income countries with established capacities and systems. However, by combining a practical, context-sensitive approach with enhanced safeguards, the potential for DPI in countries experiencing or emerging from crises should not be overlooked.

III BUILDING, SCALING, AND USING DPI

How can countries build DPI effectively and efficiently? Although DPI involves technology, it goes far beyond the procurement of a digital solution. For policymakers, this begins with adopting a holistic vision for DPI and choosing between various models for the overall architecture of each DPI system and how they will work together, as well as the role of the public and private sector. With this vision in mind, there are important implementation considerations, including assessing readiness for DPI in terms of prerequisites, considering various technology options, undertaking sometimes complex procurements for government-led DPIs, the willingness of the private sector to invest in the DPI ecosystem, and conducting pilots and user testing. These design and implementation choices should be strongly rooted in use cases across priority sectors, each of which bring their own requirements and considerations.

1. DESIGN

This section provides a brief overview of DPI architecture and core design choices and models for DPIs, and potential roles for the public and private sector depending on the type of DPI.

Overall DPI Architecture

There is no single model for the overall architecture of a country's DPI other than the requirement that various DPIs should be interoperable with each other. Although a variety of design choices and models have surfaced within individual DPIs, it remains premature to pinpoint established best practices or standard archetypes for an overarching DPI ecosystem. Successful implementation depends on selecting the approach that delivers the most impact, tailored to the local context, legacy systems, and institutional dynamics.

In broad strokes, however, countries have followed different pathways toward DPI development and adoption (Eaves 2023). Based on the country examples analyzed in Volume 2 of this report, this includes variation based on:

- **Greenfield vs. add-on:** One key variation in overall architecture is whether DPIs are built on top of existing infrastructure or from scratch. In countries with strong legacy systems, adding new functionality may be an option for quickly scaling up DPI. In other cases, legacy systems may be weak or nonexistent, and it is necessary or preferable to do a larger greenfield implementation. **Indonesia**, for example, already has a strong national ID and civil registration system, and is currently building out its DPIs by adding digital identity verification services and a mobile-based digital ID.
- **Champion and first mover:** In some cases, DPI development has been driven or championed by central government agencies, such as Ministries of Digital Transformation (e.g., **Singapore**'s Smart Nation and Digital Government Group or SNDGG) or Prime Minister's Offices (e.g., **Ethiopia**'s digital national ID). In others, they have been led by agencies, ministries, or the private sector responsible for implementing a specific DPI (such as central banks for payments DPI). In **Ukraine**, DPI efforts are led by the Ministry of Digital Transformation, supported by Chief Digital Transformation Officers and Deputy Ministers in each ministry to drive the digitalization process, as well as the National Bank of Ukraine.
- **Point of entry:** Relatedly, countries have also differed in the lens through which they approached DPI. **India**, for example, started by building a core DPI stack (beginning with digital ID, then payments and data sharing). **Estonia** began with digitalizing sectoral databases and registers to enable data sharing through X-Road/X-Tee. **Korea** started integrating databases and government services in the early 2000s, focusing extensively on interoperability and data-driven innovation. In **Australia**, the New Payments Platform (NPP) is a cornerstone of the DPI ecosystem, enabling real-time transactions through open design and public-private collaboration.

- **Public regulation vs. building:** A final difference in approach is the envisioned role of the public sector. In many cases, public authorities have led not only the definition of DPI strategies and frameworks but have been heavily involved in building and operating DPI, particularly for digital ID and data sharing. In other cases, such as many of the **European Union's** DPIs, the public sector focus has been largely on regulation and developing and maintaining common trust frameworks.

As countries progress in constructing their respective DPI "stacks," the World Bank Group will continue to document these evolving models and disseminate key innovations and lessons for implementation.[35]

Models and Design Choices for Various Types of DPI

Beyond the architecture and development of a country's overall DPI, each type of DPI—including digital identity, payments, and data sharing—has a variety of potential design choices and models. While these choices can be complex, this section distills some of the primary options for designers across core DPI systems.

Digital Identity & Electronic Signatures

The model for digital identity and e-signature DPIs varies widely from country to country, and there is no one-size-fits-all approach. Countries must make a variety of important choices—many of which are outlined in the ID4D Practitioner's Guide (World Bank 2019)[36]—including the ownership and governance of ID systems, the types of authentication mechanisms and credentials used, the type and amount of data collected, the levels of assurance and related technologies for e-signatures, and more.

Within the DPI framework, however, a fundamental decision relates to the type and number of identity providers (IDPs). For example, digital identity services can be provided by the same entity—typically a national ID or civil registration department or agency—that issues the country's foundational ID. In some cases, this is a centralized system with this entity providing the only government-recognized digital ID. In others, official forms of digital identity are provided by other entities, such as Ministries of Digital Transformation, or private partners (see Table 1). There may also be multiple IDPs operating in a federated or decentralized architecture (see below). These models are not mutually exclusive, and each offers unique

Table 1. Pros and cons of combining foundational and digital ID

Foundational ID and digital identity provided by ...	Pros	Cons
Same entity (commonly a national ID or civil registration authority)	• Reduces identity management complexity • Reduces potential redundancies (e.g., in identity proofing process) • May streamline user experience and boost inclusion (e.g., only enrolling once)	• Potential monopoly and single point of failure for identity • Concentration of identity and digital transaction data can create potential for surveillance • Traditional ID agencies may not have high digital capacity or incentives for innovation
Different entities (such as a digital ID provided by digital agency and/or other or multiple public and private entities)	• Other entities may have higher capacity to provide and innovate digital identity services • Reduces monopoly in identity ecosystem • Multiple ID providers can create competition and innovation, potentially boosting user choice and inclusion	• Added complexity to identity ecosystem with multiple stakeholders to coordinate and oversee • May take longer to develop than adding digital functionalities when reforming existing ID systems

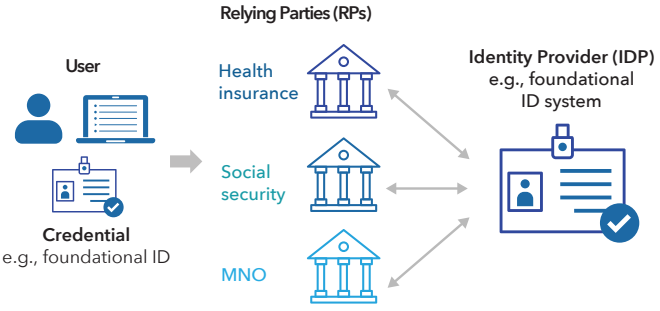
35 Helpful DPI architecture resources from other organizations include CDPI's wiki (https://docs.cdpi.dev/) and GovStack materials on broader digital government stacks, including DPI (https://govstack.gitbook.io/).

36 See, for example, a list of key design choices here: https://id4d.worldbank.org/guide/3-key-decisions-0.

benefits and challenges. Similar choices are available when developing PKI to underpin e-signatures, as described more fully in Tullis et al. (2025).

Centralized architecture has been most common for traditional foundational ID systems, such as national IDs, including those that provide digital identity services. In a centralized model, a single entity, often the government, acts as the IDP and manages and maintains the digital ID system (see Figure 15). This entity is responsible for data storage, management, and verification. Examples include **India**'s Aadhaar system and **Peru**'s National ID Card (DNI), among many others. Centralized systems can be more efficient in terms of administration and coordination, particularly in an environment with few high-capacity IDPs; can be easier to ensure compliance with legal and regulatory frameworks compared to multiple IDPs; and may also be easier to integrate with other government systems and services.

Figure 15. Single IDP in a centralized model

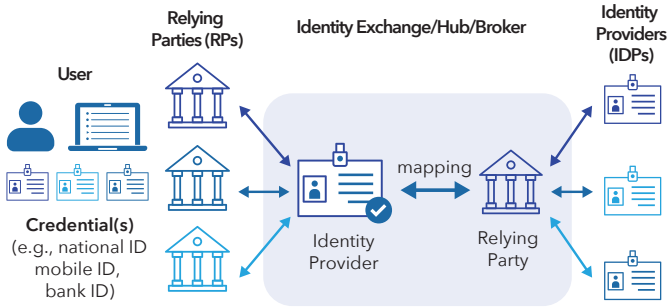


Source: Adapted from World Bank 2022b.

However, as transactions have moved online—including as part of a country's core DPI—there has been a shift toward decreasing centralization and decoupling "in person" and "online" ID. In part, this is due to some of the key limitations and risks of centralized systems, which can create a single point of failure for online authentication if they are out of service. To the degree that data storage itself is centralized, this may also increase the risks and cost of data breaches, and potential for surveillance. With notable exceptions, many foundational ID systems have provided a limited range of credential and technology options, potentially limiting consumer choice and inclusion (World Bank 2022b).

One alternative has been a federated model of digital identity. In this model, multiple public and/or private-sector IDPs operate under an explicit federation trust framework and typically implement a hub or exchange to facilitate communication between IDPs and RPs (World Bank 2022b). Examples include federated digital ID systems in **Belgium**, **Estonia**, **Italy**, and more. These models have the advantage of reducing the risk associated with a single point of failure, limiting some risk of surveillance, and providing consumer choice in their IDP and potential credential formats and form factors. They are also well adapted for establishing interoperability in digital identity and e-signatures across borders or organizations, where multiple jurisdictions need to collaborate (for example, in the **European Union**'s eIDAS framework). However, they also add complexity to the ecosystem that requires strong coordination and oversight; create challenges for ensuring the uniqueness of digital identities across IDPs; and require a high-capacity ecosystem of public and/or private-sector identity providers (such as banks, telecom operators, dedicated companies).

Figure 16. Federated model



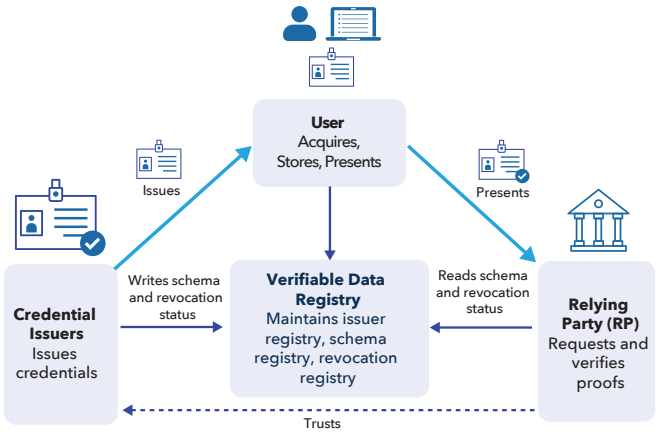
Source: Adapted from World Bank 2022b.

A third emerging model for digital identity is for users to control credentials that can be verified by service providers in a decentralized way. In a decentralized model, various public and/or private sector entities issue digitally verifiable credentials (VCs) that are stored locally by the user, typically in a digital wallet on a smartphone or smartcard. These entities can include foundational or digital ID providers, issuing VCs as an official form of digital identity (e.g., a digital national ID or birth certificate). As this model is relatively new, national-scale implementations[37] of VCs and wallets for digital identity are still limited, but relevant examples include the issuance of mobile driver's licenses in a handful of **U.S.** states, the

37 Smaller scale implementations of decentralized ID have been more common. For example, the **Kiva Protocol** initiative in **Sierra Leone** that gives unbanked people digital identities and secure control over their credit information through a decentralized approach. For more on Kiva Protocol, see: https://assets.ctfassets.net/j0p9a6ql0rn7/3jnqTBAv3MYA0ByuYC8eYr/211c7bd152a397899481b0b3ef99ab6b/Kiva_Protocol_-_Technical_White_Paper_-_June_2021.pdf.

planned **European** Digital Identity Wallet, and **Bhutan**'s National Digital Identity (NDI) wallet.[38] These decentralized models have a number of benefits, including providing users with more direct control over their identity data and when it is shared, and reducing the potential for undue surveillance. In practice, however, they also present some challenges, including operating in low-connectivity environments and those with lower levels of smartphone penetration.

Figure 17. Decentralized approach



Source: Adapted from World Bank 2022b.

As noted above, these models are not mutually exclusive, and many countries have adopted a layered approach to digital identity. For example, in countries such as **Belgium**, **Norway**, **Denmark**, **Uruguay**, and **Thailand**, government ID authorities issue a centralized identity in the form of a digitally enabled national ID card (World Bank 2022b). This credential is then used as a basis for enrolling in other digital IDs issued through federations of IDPs, or for verifying someone's identity before issuing a verifiable credential.

For e-signatures, some of the same model options apply, though model choices are linked more closely with levels of assurance. As mentioned in Section 2, e-signatures can be implemented as separate systems or coupled with digital identity. The latter is most common for high-trust e-signatures, given the strong role that identity assurance plays in e-signature levels of assurance. For example, countries such as **Argentina**, **Estonia**, **Georgia**, **Germany**, **Singapore** and **Spain** all have digital ID credentials linked to, or containing, a signing certificate based on PKI to implement strong e-signatures (Tullis et al. 2024).

Crucially, however the overall trust framework for e-signatures should enable a risk-based approach by establishing clear requirements for multiple levels of assurance. For example, in the **EU**, eIDAS provides a three-tier assurance framework,[39] that specifies requirements to meet each tier, including the processes and technologies related to the identity of the signer and the registration process; the data used for signing; the integrity of the signed document; the accreditation and supervision of the digital certificate issuer; and the device used for signing (Tullis et al. 2024).[40] For low-risk transactions, e-signatures can be implemented using multiple basic technologies, without additional requirements, as described in Table 2. However, while multiple implementations are possible for medium- and high-assurance signatures, achieving medium and advanced signatures under eIDAS requires additional processes and technologies.

Both public and private sector entities can provide e-signature solutions and underlying trust services. Many of the e-signature implementations described in Table 2 can be provided by the private sector. This requires legal and trust frameworks to ensure the interoperability of e-signatures across providers. Similarly, in most countries the underlying PKI technology to provide high-assurance e-signatures is implemented through a partnership of multiple actors, often including the private sector.[41] Where the private sector is involved, it is also common to establish a standards-based approach to governing digital ID and trust services and providing for interoperability between them, both within countries and across borders.

38 For more on mobile driver's licenses and the EU wallet, see https://www.aamva.org/topics/mobile-driver-license and https://ec.europa.eu/digital-building-blocks/sites/display/EUDIGITALIDENTITYWALLET/EU+Digital+Identity+Wallet+Home, respectively. For more on **Bhutan's** NDI, see: https://www.bhutanndi.com/ and https://trustoverip.org/wp-content/uploads/Case-Study-Bhutan-NDI-National-Digital-Identity-ToIP-Digital-Trust-Ecosystems-V1.0-2024-05-21.ext_.pdf.

39 In eIDAS terms, the levels are simple electronic signature (SES), advanced electronic signature (AES), and qualified electronic signature (QES), corresponding to low, medium, and high levels of assurance, respectively.

40 A multi-tiered trust framework is not unique to the EU, and has also been pursued by **Brazil**, **Singapore**, and other countries. However, it is not the only approach to implementing electronic signatures. Another is a technology-neutral approach taken, for example, by the UNCITRAL Model Law on e-commerce. **Australia** has also focused on the legal dimensions of e-signatures, allowing the market to determine appropriate technologies to achieve various security levels (Tullis et al. 2024).

41 For more on PKI architecture, see Tullis et al. 2025.

Table 2. eIDAS levels of assurance for electronic signatures

Level of Risk / Assurance	Implementation examples	Process & technology requirements
Low	• Typing a name at the end of an email or document • Clicking on an "I accept" button on a website • Using a scanned image of a handwritten signature • Using a finger or stylus to hand write a signature on screen • Digital authentication (for example, a biometric or a one-time password)	None.
Medium	• Plug-ins to PDF reader applications that allow digital certificate-based electronic signing • Cloud-based signature solutions offering a secure remote signing service • A mobile app using secure elements in smartphones to generate signatures • A hardware token, such as a smart card containing a digital certificate on a chip.	• *Identity of the signer:* Electronic signature uniquely linked to a signatory identity, e.g., through ID document verification. • *Registration process:* Requires some assurance of the identity of the signatory (e.g., ID verification), but no requirement for in-person. • *Data used for signing:* Must be under the sole control of the signer (e.g., Digital authentication using a biometric or other factor required for each signing transaction). • *Integrity of signed document:* Cannot be modified after signing. • *Supervision of digital certificate issuer:* Ex-post.
High		*The above, plus:* • *Registration process:* Rigorous in-person or equivalent onboarding with a high-trust ID. • *Data used for signing:* Must also conform to rigorous standards for digital certificates • *Accreditation of digital certificate issuer:* The signature solution vendor is accredited as a qualified trust service provider (QTSP) by the competent Supervisory Body before issuing the digital certificates used in its products. • *Device used for signing:* High-security, certified signature-creation device required (can be physical or in the cloud). • *Supervision of digital certificate issuer:* Ex-ante.

Source: Adapted from Tullis et al. (2024).

Payments[42]

The Fast Payment System (FPS) ecosystem and design choices

The FPS ecosystem is a complex network that includes various key stakeholders working together to facilitate seamless transactions. At the core is the central bank, which often oversees and regulates the system to ensure safety, efficiency and reliability. In some cases, other regulatory bodies may also be involved. The operator is responsible for the day-to-day management and technical operation of the payment system. Ownership can vary, with some systems owned by the central bank, consortia of banks, or private entities. Participants in the ecosystem include banks and non-bank payment service providers (PSPs) that directly interact with the payment system. Third-party providers, such as technology vendors and financial intermediaries, offer essential services that enhance functionality and user experience. End users, comprising individuals, merchants, and government agencies, are the final beneficiaries, using the system for transactions like merchant payments, person-to-person transfers, and bill payments.

Designing and implementing an FPS involves making several critical choices that span various aspects and that affect each participant of the ecosystem. Each choice will contribute to the overall success and efficiency of the system. These decisions include, determining the objective, the stakeholders involved, access to the system and accordingly the participation model for both banks and non-bank payment service providers (PSPs), selecting the appropriate clearing and settlement models, and identifying the most effective payment instruments, use cases and access channels. Furthermore, the integration of overlay services, such as aliases, can significantly enhance user experience and adoption rates. Technical aspects and specifications, such as the type of messaging standards, are also critical to the effectiveness of an FPS.

Public authorities' role

Public authorities, especially central banks, play a crucial role in maintaining the safety, efficiency, and competitiveness of retail payment systems, including payment DPIs like FPSs. Their responsibilities involve ensuring that payment systems are accessible and effective while also protecting consumers and fostering a competitive landscape. To achieve these objectives, central banks take on various roles: operational, catalyst, and regulatory. In their operational role, they may provide settlement services or directly manage certain payment systems. Acting as catalysts, central banks work closely with banks and non-bank payment service providers to enhance payment infrastructure and drive the development of new services. In their regulatory role, they monitor and evaluate retail payment systems, even in cases where explicit legal authority is lacking, using regulation and active engagement with market participants to guide system improvements.

Public authorities have a crucial role in the development and oversight of FPSs in many jurisdictions. They are often involved from the initial stages of planning, providing strategic guidance and integrating an FPS into broader national initiatives, as seen in countries like **Thailand** and **Brazil**. Even when the private sector leads these efforts, public sector influence remains significant, with central banks acting as key drivers for the design and implementation of these infrastructures. Central banks also oversee an FPS to ensure safety and efficiency, requiring operators to manage various risks and comply with regulations. Operational roles differ by country; some central banks, like in **Mexico**, fully own and operate the FPS, while in others, responsibilities are shared with private entities. Across all models, public authorities work to align the FPS with objectives of stability, efficiency, and financial inclusion.

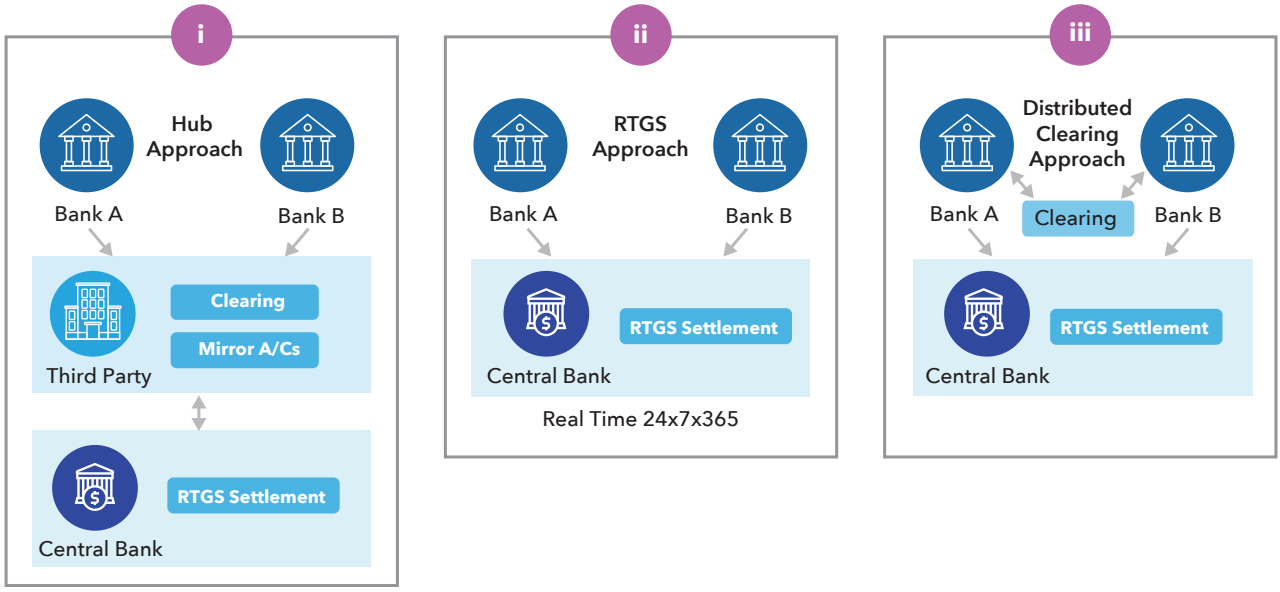
When public authorities operate an FPS, it is essential to implement safeguards to ensure the private sector is not crowded out. Public authorities can achieve this by adopting a minimalistic design that allows the private sector to develop additional services on top of the FPS, such as merchant payments. Additionally, key overlay services, such as end-user access channels, can be developed by the private sector. Furthermore, public authorities can enable interoperability between different private sector solutions to enhance economies of scale and network effects, thereby increasing the benefits of DPIs for both market participants and users.

Participation

The success of FPS depends on the participation of both banks and non-bank PSPs, with regulatory incentives often needed initially to encourage their involvement. FPSs can have either direct or a combination of direct and indirect participants. Direct participants, typically banks, have a direct link to the payment system infrastructure and a settlement account at the central bank. The non-banks could be direct or indirect participants based on the technical capabilities and access to central bank account. Indirect participants, such as other

42 This section is adapted from the World Bank's FASTT Flagship report (World Bank 2021b).

Figure 18. Types of clearing models in FPS



Source: World Bank 2021b.

financial institutions or PSPs, use the infrastructure through a sponsor bank's settlement account (even though they may have direct technical connectivity to the FPS). Jurisdictions adopt various access models for non-bank PSPs: indirect participants sign commercial agreements with direct participant banks (e.g., PromptPay in **Thailand**, Pix in **Brazil**); direct participants maintain their own settlement accounts at the central bank (e.g., RPP in **Malaysia**, **SPEI** in **Mexico**); and some non-bank PSPs connect directly to the infrastructure but settle through a commercial bank (e.g., UPI in **India**).

Clearing and Settlement

There are three main clearing models for FPSs. The hub approach, used in **India**, **Singapore**, and the **UK**, involves a clearinghouse managing real-time clearing, with its participants bound by the rules of participation, and downstream settlement with the central bank. The RTGS-based approach, adopted by **Mexico** and the **USA**, uses the RTGS system for clearing and settlement, returning failed payments to the originator. The distributed clearing model, followed by **Australia**, allows participating banks to validate and clear payments in real time on a 24/7 basis, with the payer bank initiating settlement with the central bank.

The choice of a settlement model significantly impacts safety and efficiency in fast payments. There are primarily two main settlement models: deferred net settlement (DNS) and real-time settlement. In the DNS model, inter-participant obligations are settled on a net basis at the end of a predefined cycle, either once or multiple times a day. This model is more efficient as it reduces liquidity needs, but it carries inherent risks such as credit risk from net debit positions, which must be managed with measures like debit caps, guarantee funds, prefunding, and collateral arrangements, etc. In contrast, the real-time settlement model involves continuous, order-by-order settlement of funds. A fast payment transaction is completed only if the originating participant has sufficient balances in its settlement account with the central bank or other settlement agent, eliminating credit risk between participants and providing immediate finality of all payments.

Key technological options and specifications

Technological options and specifications for FPSs include the choice of messaging formats and integration methods to streamline electronic data exchange and enhance transaction efficiency. Messaging formats are standards for electronic data exchange between institutions in a payment system, covering categories such as orders, invoices, customs documents, remittance advances, and payments. Uniform messaging standards are essential for standardizing payment flows, especially with the rise in cross-border transactions and multiple payment systems. These standards facilitate the identification of senders and receivers, specify key attributes of a payment transaction (such as currency, amount, and value date), and include additional information necessary for the

onward transmission and processing of transactions. The main messaging standards for domestic payment transfers include ISO 8583, SWIFT MT Standards, and ISO 20022, with some operators developing their own proprietary standards. **Australia**, the **EU**, **Poland**, **Singapore**, and **Thailand** have adopted ISO 20022. **Bahrain**, **Chile**, **China** and **Hong Kong SAR China** adopted ISO 8583. India uses proprietary standards (ML-UPI), with plans to migrate to XML and ISO 20022. **Mexico** and **Nigeria** use proprietary standards (Binary and XML, respectively).

A key technological choice for FPSs involves how participants and the infrastructure integrate and interact. APIs facilitate seamless integration between financial institutions and service providers, enabling real-time transactions and enhancing user experience. Other integration methods, such as file-based batch processing and direct database access, involve more complex and limited real-time interactions. APIs boost interoperability by providing easy access to fast payment arrangements and various banking functions, including account details and lending. They also enable interactions between stakeholders, such as third-party application providers and consumers, supporting payment initiation, e-commerce transactions, and other applications. Fast payment operators typically define the API framework, outlining essential attributes for system integration. **Australia**'s NPP API framework aligns with ISO 20022 and encourages the use of its capabilities, though it is not mandatory. **India** uses standardized APIs exclusively for UPI payments, supporting extensive third-party integration and customer account aggregation. **Mexico** offers limited APIs through Banco de México for value-added services like transaction status checks and retrieval, with plans to expand access to third-party open APIs. Under the **United Kingdom**'s Open Banking framework, developed by the Open Banking Implementation Entity (OBIE), the Financial Conduct Authority (FCA) grants licenses for various services such as payment initiation and account information, covering both technical and non-technical aspects, including customer experience guidelines, dispute management, and API security specifications.

Data Sharing

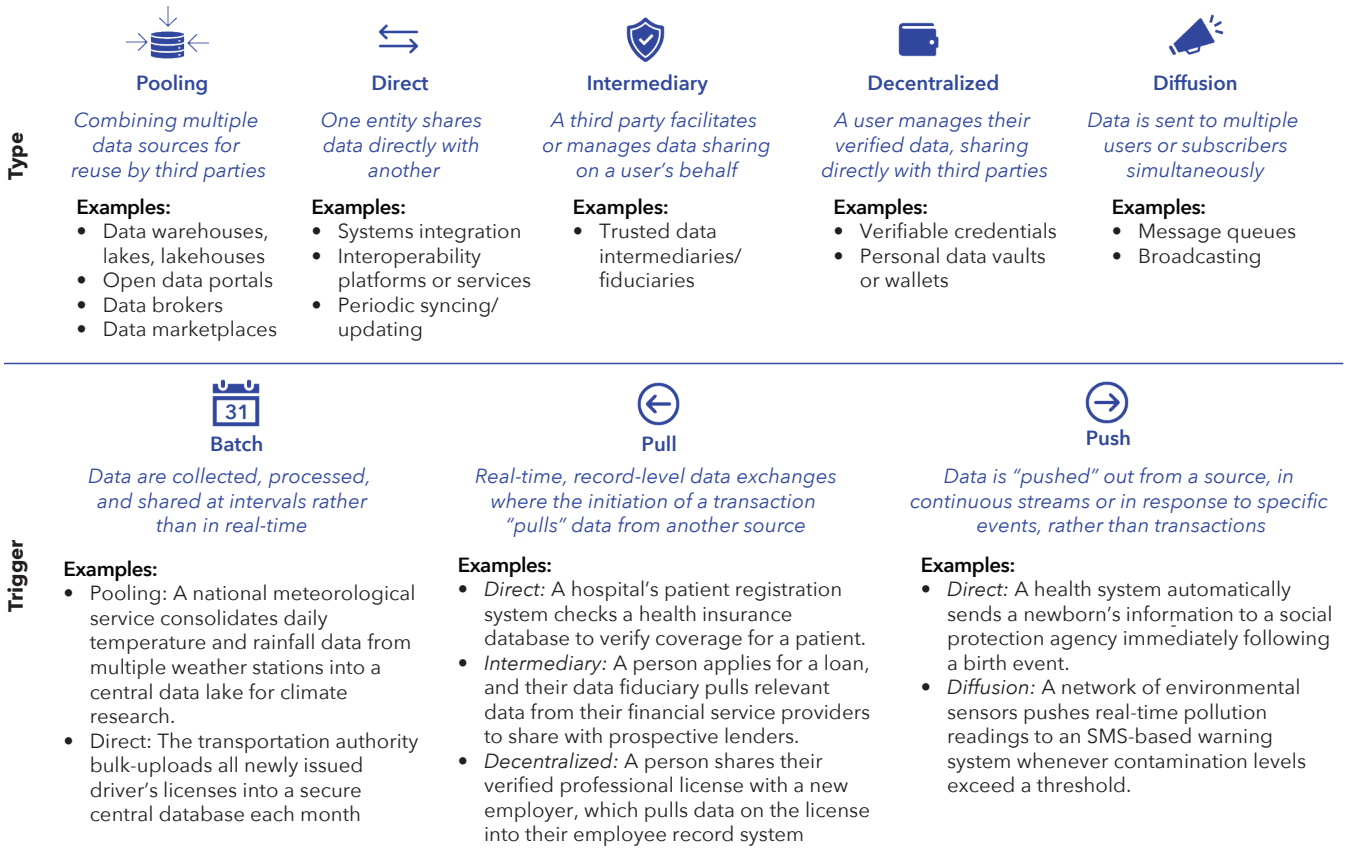
The appropriate model for a specific data sharing system varies significantly by use case, including the nature of the data involved and the purposes for which it will be used—and multiple systems are likely required. Not all data is created equal, and the methods chosen to share it must reflect its sensitivity and intended usage. For instance, personal or sensitive data necessitates strong privacy protections to prevent oversharing, while open or public-interest data may require mechanisms to ensure it is adequately shared and accessible. Factors such as the type of entities involved public institutions, private companies, individuals), the legal and regulatory frameworks governing the data, and the intended application of the data (such asanalytics, transactions, public services) all influence the appropriate data-sharing method. As such, most countries are developing multiple data sharing systems.

Selecting the right method for a particular use case requires careful consideration of the specific risks, whether they pertain to data integrity, privacy, availability, or regulatory compliance. The risk of over-sharing sensitive data often calls for strong privacy controls, user consent mechanisms, and strict access management. Conversely, the risk of not sharing critical public-interest data can result in missed opportunities for societal benefits and necessitates strategies to enhance availability, discoverability, and interoperability. The balance between these concerns is often in tension, meaning that systems designed for data sharing must be tailored to the specific requirements of each use case. A one-size-fits-all approach is ineffective, and trusted data-sharing frameworks must be adaptable to meet the diverse needs of different scenarios.

There are several methods by which data can be shared, each suited to different use cases and requirements. This section discusses a few of the most common for DPIs, summarized in Figure 19. This includes various types of methods, including data pooling, direct sharing, intermediated data sharing, decentralized credentials and documents, and data diffusion. These approaches can involve multiple "triggers" for data sharing, related to the impetus, direction and frequency of data sharing, including batch data transfers at specific intervals, transaction-based "pulls," and event-based or continuous "pushes" of data from source to recipient. These various methods, along with related requirements, enablers, and architectures for data sharing are discussed in more depth in Tullis (forthcoming).

Direct data sharing methods are among the most common ways digital data is shared, particularly among government entities. Direct data sharing can be implemented via direct integrations between two systems (such as a civil register and an ID system), as well as interoperability platforms and services (such as **Estonia**'s X-Tee/X-Road and **Singapore**'s APEX). Data sharing between these systems can be processed in batches (for example, nightly syncs) or in real time via pull-requests triggered by specific transactions (such as hospital system pulling data from an insurance provider's system on a patient's coverage), or pushes triggered by specific events (such as a hospital system notifying a civil register system at

Figure 19. Data sharing models



Source: Adapted from Tullis (forthcoming).

the event of a new birth). In general, bilateral integration is not feasible as the number of digital systems involved grows; interoperability platforms and services can help centralize the governance of data sharing while federating or decentralizing data sharing and management. This is because in typical interoperability platforms, data flows directly from the source to the recipient, without requiring data to be processed by a central intermediary.

Pooling is another important data-sharing method that involves centralizing data from multiple sources for analysis or dissemination by a third party. This includes data warehouses (typically structured data, processed for analysis), data lakes (often unstructured data or a mix, stored in its original format), and data lakehouses (a mix of processed structured data and unprocessed unstructured data). It also includes open data portals with data published for public consumption, data marketplaces where data providers can list datasets for purchase or access. The pooling approach is particularly useful for policy planning, large-scale analytics, and open data initiatives where data from various entities are combined to provide a comprehensive overview. While pooling is powerful for enabling insights from diverse datasets, it poses challenges related to standardization, data quality, and privacy—especially when sensitive information is involved. Data must be carefully processed and sometimes anonymized before aggregation to protect individuals' privacy while still enabling meaningful analysis.

Intermediated methods involve third-party platforms or entities that facilitate data exchange on behalf of individual data subjects. Although intermediated methods also involve third parties like the pooling method, they differ in two ways. First, pooling methods tend to operate through batch sharing, while intermediated methods typically pull data at the individual- or record-level for a specific transaction. Second, the role of the third-party intermediaries—sometimes called data fiduciaries—is to act on behalf of the data subject, ensuring that their data is shared in a controlled manner and in their interests. These methods can help ensure that data sharing adheres to regulatory requirements and that trust is maintained between parties. Examples of this method include regulated schemes such as **India's** Data Empowerment and

Protection Architecture (DEPA) or the **European Union**'s Data Governance Act.

Decentralized methods place individuals at the center of data sharing, giving them greater control over how their personal data is accessed and used. Common in the analog world—where individuals often present ID cards and paper documentation to obtain a service—decentralized data sharing is only beginning to take hold in the digital world. This model is exemplified by digital verifiable credentials (VCs), personal data vaults, and other consent-based data sharing systems. In this approach, the individual has a direct role in managing their data, deciding who can access it and for what purposes. This method empowers individuals without relying on intermediaries or central authorities. The recent revision to the **European Union**'s eIDAS regulation (discussed above in the context of decentralized identity) exemplifies this approach by allowing individuals to store and control their digital IDs and other credentials securely in a digital wallet. This model is gaining momentum globally, as evidenced by the adoption of similar frameworks elsewhere, such as in the **African Union**.

Finally, diffusion methods involve the constant or near-constant exchange of data, often through streaming platforms or event-driven broadcasting. These methods are ideal for applications that require real-time data processing, such as Internet of Things (IoT) networks, smart city infrastructures, disaster early warning systems, or public utilities management. Continuous methods ensure that data flows smoothly and consistently between systems, allowing for instantaneous updates and dynamic responses to changing conditions. Event-driven models, such as message queues and brokers, allow for scalable and reliable data sharing by decoupling the sender and receiver systems, ensuring data is shared asynchronously and processed as needed without immediate demands on either party's systems. These methods are critical in scenarios where timely data processing and responsiveness are key, such as traffic monitoring, customs and border procedures, or emergency response systems (Tullis, forthcoming).

Role of the Private Sector

Successful DPIs typically have high levels of use by the private sector. For most people, touchpoints with government service providers are much more infrequent than with the private sector. Thus, while government services providers and other public authorities are often the first users of DPIs (such as via e-service portals), the sustainability of DPIs is typically achieved when companies have integrated DPIs into their business processes (for example, using a digital ID for onboarding new customers or a fast payment system to collect fees from customers).

However, the private sector has a broader role to play in developing and deploying DPI, bringing resources, expertise, and innovation to the table. While the public sector plays an essential role in DPIs—as potential DPI providers, but also through strategies, regulations, standards, and oversight—it is equally important to harness private sector innovation and avoid crowding out markets in DPI development. Beyond their role as vendors that provide the technology and infrastructure for DPI development. Furthermore, private companies can contribute to innovation and development of DPIs by building upon foundational rails and regulations provided by governments. They can create new applications and services that leverage DPI, leading to a thriving ecosystem.

As the DPI landscape evolves, it is likely that the models for private sector involvement will continue to adapt. For example, innovations in data sharing DPIs and the need to develop new ways to meaningfully provide people with control over their data—without overwhelming users with "consent popups"—are leading to new models of data "fiduciaries" or intermediaries (described above). This creates a potential area of growth for the market, and there are already multiple private-sector and non-profit-led organizations operating in this space (Desai et al. 2022).[43]

The right balance for public and private involvement in DPIs also depends on the specific DPI and country context. The opportunities for private sector involvement will vary significantly for each country, for different DPIs, and likely over time. For example, public authorities are likely to continue playing a strong role when it comes to issuing legally recognized forms of digital identity, although there are still ample opportunities for public-private partnerships and a broader market for private-sector provided digital identity. Jurisdictions like the **EU** and **India** that already have highly developed IT sectors have focused on regulation and crowding in private sector participation for personal data sharing DPIs, but this may not be immediately feasible in contexts with fewer market players.

43 This includes, for example, Inrupt, Digi.me, and the Data Transfer Project.

Table 3. Potential role of private sector in DPI

Type of DPI	Vendor	Provider or Operator	User (Relying Party)
Digital Identity	ID software and applications vendor and integrator, biometric systems, enrollment devices and hardware.	Provide and/or operate digital authentication and credential systems, apps, and/or services; serve as digital identity providers (IPs) within a trust framework; provide/operate digital wallet infrastructure; participate in standards development.	Use digital ID services provided by government and/or a private company.
e-signatures	Suppliers of e-signature software, public key infrastructure (for higher levels of assurance), cryptographic tools, security services, secure devices, and other software and hardware underlying the provision of e-signatures.	Provide and/or operate e-signature services and/or related trust services including the underlying technical implementation of digital signatures and digital certificates.	Rely on e-signatures provided by government and/or a private company by integrating their creation and verification into business processes and service-delivery workflows.
Digital Payments	Software vendor, integrator, and operator; payment instruments and access points and channels, such as points-of-sale; provision of switching, clearing and settlement services; provision of value-add and overlay services, such as fraud detection tools.	Operate payment networks, monitor real-time transactions, ensure interoperability and manage clearing and settlement. Payment services provider for end users; merchant acquiring and specialized merchant services such as aggregation and facilitation services.	Use different types of payment services including person-to-person and merchant payments, bulk payments and international remittances.
Data Sharing	Provide data exchange platforms, software, and associated systems integration services; provide data processing and transformation tools; provide security solutions such as encryption and access-control mechanisms; conduct audits and conformity assessments.	Provide and/or operate data sharing platforms or data streaming services; act as data intermediaries or brokers; provide/operate digital wallet infrastructure; participate in standards development.	Use shared data to generate insights, improve decision making and offer predictive services.

Building Trust

For DPI to fulfill its promise of increasing online trust, it is essential to ensure the trustworthiness of DPI systems. This can involve a variety of steps, including those described below, such as conducting and publishing comprehensive legal and regulatory reviews; privacy and rights impact assessments; using widely recognized standards for technology, policy, and regulations; prioritizing underserved groups; strategic communication and consultation with stakeholders; effective grievance redress mechanisms; and more. These steps should be integrated into the design phase of DPIs and continued throughout implementation.

To begin, designing a new DPI requires a comprehensive assessment of existing legal and regulatory frameworks and governance mechanisms to ensure compliance and to safeguard the rights of stakeholders. These frameworks—as discussed in Section 2—are essential to establish the legal boundaries within which DPIs operate, providing requirements on data privacy, digital transactions, cybersecurity, and intellectual property rights. Assessing regulatory frameworks involves examining national and international requirements, understanding their applicability to digital platforms, and identifying gaps that need to be addressed to facilitate the development of DPI without compromising security or privacy.

The adoption of recognized standards can make the implementation of DPI more efficient and transparent, building trust. Using widely accepted policies, standards, and frameworks can help signal the legitimacy of the project and simplify development, integration, and operation and promote interoperability between different systems and platforms, reducing the need for costly and time-consuming customizations. This consistency can also streamline procurement, lower implementation risks, and facilitate collaboration among various stakeholders.[44] In contrast, adopting custom policy and regulatory solutions often leads to increased complexity, higher costs, and potential compatibility issues, slowing deployment and making maintenance and operation more challenging and costly. Standards also enhance scalability and adaptability, allowing DPIs to evolve with technological advancements and changing user needs.

Prioritizing inclusivity and accessibility is essential for building trust in DPI. Inclusivity ensures catering to all segments of the population, including potentially marginalized and vulnerable groups, such as women and girls; low literacy groups; remote and rural dwellers; the elderly; persons with disabilities; refugees and migrants; internally displaced persons; stateless groups; ethnic, linguistic and religious minorities; and sexual orientation and gender identity (SOGI) minorities, among others. This includes designing platforms and building blocks that adhere to open standards and specifications around universal accessibility, ensuring that in-person access points (such as digital ID registration) are accessible to all, user-testing groups and others who are more likely to be affected by the digital divide, and engaging in dedicated outreach, education, and consultations with marginalized and vulnerable people and advocacy groups.[45]

Engaging a diverse set of stakeholders in the design process is key to success. Multi-stakeholder consultations should involve a wide range of participants, including government entities, private sector, academia, and CSOs working on technology, privacy, rights, and development. Co-creation, where stakeholders collaborate to design, develop, and refine DPIs, can foster a sense of ownership and increases the likelihood of successful implementation and adoption. Regular consultations can also help in identifying potential challenges early in the process, addressing opposition, enabling proactive solutions.[46] For instance, **Ukraine**'s Diia platform, which supports digital ID verification, e-signatures, and document storage, was developed through collaboration between government, technologists, and civic innovators.

To encourage adoption and participation in DPIs by the public at large, effective communications and skill building are essential. DPI as an abstract concept and unknown to the public at large. Therefore, developing clear understanding and communications around potential benefits of specific DPIs—such as cost reductions for online service delivery, lower administrative fees for online company registration, improved access to essential services, or enhanced user experiences through proactive approaches to service delivery—is important to build understanding and trust. Providing transparent communication that emphasizes how to use DPIs safely and which security and privacy safeguards are in place can also help encourage trust and adoption. Additionally, offering positive incentives, as well as meaningful sanctions for non-compliance, are important for boosting adoption of policies and good practices (such as data privacy and security standards) among government and private sector users.

Grievance redress mechanisms (GRM) are crucial for ensuring accountability. Key elements of a good GRM system include easy accessibility through multiple channels (web, mobile), efficient handling of grievance cases with automated routing, and proactive communication. The GRM should also prioritize data protection, transparency, and inclusivity. For example, the Digital **Malawi** project's GRM is founded on principles of accessibility, predictability, confidentiality, fairness, and transparency, designed to include marginalized and vulnerable populations.[47] Effective GRMs address user concerns and provide valuable insights for continuous improvements.

44 OECD (2020), "The OECD Digital Government Policy Framework: Six dimensions of a Digital Government", OECD Public Governance Policy Papers, No. 2, OECD Publishing, Paris, https://doi.org/10.1787/f64fed2a-en.

45 See, for example, ID4D notes on inclusion for persons with disabilities (World Bank 2020) and SOGI groups (Lebbos et al. 2021).

46 See, for example, the ID4D Guide on CSO Consultation (Eichholtzer 2022).

47 For more information on the Digital Malawi GRM, see https://digmap.pppc.mw/home/grievance-redress-mechanism/.

2. IMPLEMENTATION

This section provides an overview of key topics related to DPI implementation, including potential prerequisites that should precede or accompany DPI rollout, adoption of open-standards, considerations for using open source, DPI procurement, and conducting pilots and user testing.

DPI Prerequisites

As a country or jurisdiction develops its DPIs, several critical elements are needed to ensure successful design, deployment and adoption. While some of these might be developed in parallel with DPI, it is essential to have these elements in place once the infrastructure is deployed to ensure the safe, inclusive, sustainable, and empowering outcomes that are pursued. These prerequisites include:

- **Political Commitment:** There must be a strong and sustained commitment from leaders and policymakers. This commitment should manifest in the form of clear visions, strategies, and the political will to drive DPI initiatives forward.
- **Stakeholder Engagement:** It is important to engage with a wide range of stakeholders, including various ministries, departments, agencies, and other public authorities, private sector, civil society, academia, and end users to leverage their expertise and ensure that the DPI meets the diverse needs of the society and has widespread support.
- **Institutional and Technical Capacity:** Public institutions must have the capacity to effectively govern DPI initiatives, and DPI implementers—whether in the public or private sector—must have the technical capacity to effectively implement and manage them. This includes having and retaining skilled personnel and effective processes in place for the development, operation, or oversight of DPIs.
- **Legal and Regulatory Framework:** A comprehensive legal framework should be established before or in parallel to DPI development to address issues related to data protection, privacy, cybersecurity, and digital transactions.
- **Connectivity Infrastructure:** Robust and widespread internet connectivity is essential, as it forms the backbone of any digital infrastructure. This includes both the physical broadband and wireless networks, as well as policies that make internet and digital device access affordable and equitable.
- **Digital Access and Literacy:** The population needs access to digital devices and the internet. Equally important is digital literacy, ensuring that people have the skills and confidence to use digital services safely and effectively.
- **Financial Resources:** Adequate funding must be secured for both the initial development and the ongoing operation of the DPI, whether provided by the public or private sector.
- **Private Digital Ecosystem:** A vibrant private digital ecosystem—including businesses, startups, and entrepreneurs—is crucial to help innovate and create value by leveraging the DPI.

How to develop and sequence these requirements is beyond the immediate scope of this paper but will be expanded in future work. In addition, there are many quality resources that provide in-depth guidance on specific topics, including connectivity, legal and regulatory frameworks, and stakeholder engagement.[48]

Open Standards

Open standards are a critical enabler for building successful and sustainable DPI. They promote interoperability, reduce vendor lock-in, and reduce barriers to leveraging DPIs as building blocks, making them more accessible. Open standards can reduce the risk of certain types of vendor lock-in by enabling countries to switch providers more easily if needed and to easily adapt the technology to changing needs. Open standards are also essential for enabling cross-border use of DPIs, such as mutual recognition of digital IDs, interoperable fast payment systems and secure data sharing. They can lower the costs and risks associated with international transactions. Examples of open standards for digital identity can be found in Mittal (2022); Box 6 provides examples in fast payment systems.

48 For example, visit the World Bank's Digital Transformation website (https://www.worldbank.org/en/topic/digital) for resources on broadband infrastructure, and the ID4D website for the ID4D Practitioner's Guide, ID Enabling Environment Assessment (IDEA), and additional publications on CSO and stakeholder engagement.

Box 6. Open standards in fast payment systems

Messaging standards define the syntax, structure, and semantics of messages exchanged between parties. In FPS, these standards are essential for ensuring a common understanding of transmitted data across linguistic, regional, or system boundaries. Implementing a messaging standard guarantees that the exchanged data is correctly interpreted and machine-readable, leading to cost reductions and increased efficiency. Furthermore, messaging standards define the fields and data elements that compose a message, which can be utilized for various use cases. Globally, three main types of messaging standards are used in FPS: ISO 8583, ISO 20022, and proprietary.

The International Organization for Standardization (ISO) has defined various standards for facilitating financial transaction messages, evolving with payment dynamics and technological advancements:

- ISO 8583, designed for high-volume, low-latency payment instructions, is widely used for card payments (ATMs and point-of-sale terminals) and supports pull payments, particularly for auto-debit mechanisms. However, its unstructured format limits information exchange and customization.
- ISO 20022 offers greater flexibility with structured, data-rich exchanges and allows the standardization of messaging components, emerging as the global benchmark for real-time payments.
- Proprietary messages can be XML-based, like ISO 20022 messages, or non-XML-based, such as ISO 8583 or SWIFT MT messages. These messages offer high levels of customization and can leverage the experience and resources of a payment system implementer, leading to the development of common platforms and reduced user training requirements.

A comparative analysis of messaging standards using both quantitative and qualitative methods highlights their different strengths and weaknesses. ISO 8583, with its unstructured fields and smaller size, is ideal for environments with limited infrastructure but lacks updates and fields necessary for advanced operations and reconciliation. ISO 20022, the global standard for electronic messaging between financial institutions, supports both structured and unstructured data, offers greater data-carrying capacity, and undergoes regular updates, making it suitable for robust network environments and enhancing interoperability. For this reason, many operators using ISO 8583 aim to migrate to ISO 20022, necessitating clear business requirements, market practices, and a migration roadmap to share information between financial institutions effectively.

Proprietary payment messages are unique formats defined by a country, region, or monetary authority to facilitate payments. These formats are typically localized and require widespread adoption throughout the payment ecosystem to be effective. Due to customization for specific regional needs and local languages, they often lack standardization for cross-border payments. However, this can achieve interoperability with middleware, making them ideal for niche requirements where flexibility is prioritized.

Source: Adapted from World Bank (2021b) and World Bank (2022d).

Technology Choices

Beyond standards, there are several high-level technology choices in DPI development. For example, countries can choose between proprietary or open-source software solutions as the basis for building specific DPIs, with important tradeoffs that should be assessed for each country context. There are also high-level architectural choices related to emerging technologies, such as implementing verifiable credentials and wallets, that can affect how these systems are used. In general, technology should be selected through careful consideration of country context, inclusive of the available capacity, resources, and appropriateness for priority use cases. By carefully considering these technology choices—and prioritizing outcomes and architecture over specific solutions—policymakers can build robust and resilient DPI that not only meets current needs but also adapts to future challenges.

Open-Source Software

DPIs can be built using customized open-source software (OSS), though OSS is not required. While open standards include publicly available guidelines or specifications to ensure interoperability and compatibility between different systems and products (often developed through consensus by standard-setting bodies), OSS makes the actual software code open and freely available for any organization to use and customize. Although OSS adoption still requires procuring system integrators, in addition to hardware, devices, and other IT services, it can potentially lower the up-front cost of DPI software and shorten the road to piloting and testing. OSS can also facilitate reuse of technology across borders. For example, Estonia has made the underlying technology for its X-Tee data exchange platform available as an OSS (X-Road), which has been used or has inspired countries like **Ukraine**, **Cambodia**, **Finland**, **Mauritius**, **Kyrgyz Republic**, and **Namibia**. This demonstrates how OSS can be used to share knowledge and best practices, fostering innovation and adoption of DPI globally.

Experience has shown that implementers need strong capacity to manage the development of DPI using OSS. Whether integrated in-house or with support from a systems integrator, the use of OSS that may be unfamiliar to the development team can bring additional risks and learning curves. A key lesson from past DPI implementations using OSS shows the importance of having detailed and accessible documentation and a viable market ecosystem, including of systems integrators and providers of peripheral devices and software that work with the software solution. Sufficient Internal capacity to manage OSS deployments is also important. In every case, it will be important for the country to assess the pros and cons of adopting OSS for DPI, including total costs, time to deploy, and potential lock-in risks as part of a detailed market analysis.

Verifiable Credentials and Wallets

Verifiable credentials (VCs) and digital wallets are a specific architecture for digital identity and sharing personal data and documents. As described above, VCs enable digital issuance and verification of specific attributes such as a person's identity or credentials such as educational certificates, business permits, employment information, vaccine certificates, and more. Digital wallets—akin to physical wallets—offer a user-friendly and secure means for individuals to store, manage, and present their credentials. Compared with physical wallets, however, they provide higher levels of security (for example, using selfie authentication to ensure that the person using the wallet and credential is its true owner) and can offer additional features to protect data (such as the ability to selectively disclose certain attributes only).

By putting the user in control of credential management and use, VCs offer a new architecture for how people manage their personal information digitally. Through a decentralized use, people can directly attest to their identity or data through presentation to a service provider, without the involvement of the credential issuer (for example, a national ID agency, ministry of health, or university), reducing the potential risk of profiling that comes with centralized systems for authentication or data exchange. For this reason, the past five years have seen multiple prominent developments in the VC/wallet space, including maturing standards—such as W3C and OpenID standards ISO/IEC standards for mobile driver's license (mDL) and online credential registration and KERI for legal entity identification—large-scale rollouts in multiple **US** jurisdictions for mobile driver's licenses and the **European** Digital Identity Wallet. Countries like **Bhutan** and **Korea** are implementing VCs and wallets as their main form of digital ID, while **Thailand** is piloting VCs for people to manage and share their education transcripts.

Still, this technology is not appropriate for all types of digital identity or data sharing applications or contexts. For example, some data sharing applications such as aggregating or warehousing open data or sharing of non-personal data between entities require different technologies. In addition, the most advanced VC/wallet standards rely on smartphone technology which is still not accessible to billions of people. For this reason, countries such as **Cambodia**'s Verify.Gov.Kh service uses a hybrid approach that includes paper-based versions of VCs with 2D barcodes that users can print themselves.

Procurement

Procurement is a critical challenge for DPIs and other digital services built by public authorities and can present significant challenges. One major concern is vendor lock-in, where countries become overly reliant on specific vendors. This can lead to high costs, limited interoperability, and difficulty adapting to evolving needs. To address this, countries should prioritize building local technical and operational capacity, adopting open standards, and consider investing in modular designs that enable swapping out underperforming components or vendors without having to rebuild the entire system.

Another challenge for government-led DPI is the capacity to manage procurement and contracts effectively, especially given the fast-evolving nature of relevant technologies. This

can result in lengthy timelines, suboptimal contract negotiations, and a lack of oversight. To overcome this, governments should invest in training and development for procurement professionals, streamline processes, and consider using data-driven approaches to identify and evaluate potential vendors. By addressing these procurement-related issues, countries can ensure that DPI projects are implemented efficiently, and sustainably. Efforts to certify solutions according to specific standards or specifications can improve the information available and help countries avoid some pitfalls.[49]

There are several good practice examples related to public procurement in the digital space. For example, governments in **Australia**, **Singapore**, and the **UK** have developed dedicated online marketplaces for the procurement of not just commercial off the shelf software (COTS), but also subscriptions and services that have been pre-negotiated and can be purchased based on framework agreements, such as cloud computing resources and software development. Still, more work is needed in the DPI procurement space to reduce costs, shorten procurement timelines, address capacity and lock-in issues, and spur market innovation. While funding from donors and development partners can help with start-up costs, ensuring longer term sustainability is essential for the adoption and impact of DPIs.

Pilots and User Testing

Pilots and user testing are integral to a human-centered design approach and can greatly enhance the success of DPI implementation. These preliminary steps allow for the practical evaluation of the system in a controlled, real-world environment, providing valuable insights into user experience and system performance. By incorporating diverse user feedback during these stages, governments can ensure that the DPI not only meets technical specifications but also aligns with the actual needs and expectations of people and service providers. This iterative process creates a feedback loop for continuous improvement, fostering the development of a system that is not only functional but also user-friendly and responsive to the public's needs.

In Indonesia, for example, the Directorate General of Population and Civil Registration (Dukcapil) developed a mock digital ID application and tested it with women, low-literacy groups, and persons with disabilities across the country. This design process was done to help ensure the future user interface and features would be accessible and user friendly for vulnerable populations. The findings and recommendations from this testing—such as the need to retain offline/in-person onboarding processes, develop the application to make use of operating system-native talk back, and simplify navigation—are being adopted and rolled out in late 2024.

Incorporating ongoing feedback mechanisms as systems are deployed can also ensure continuous improvement. For example, robust monitoring and evaluation systems, and periodic client satisfaction surveys can provide important insights to course-correct and address urgent issues. This approach not only enhances public engagement but also ensures that digital services remain aligned with the evolving needs of users.

3. SERVICE USE CASES

Realizing the potential of DPI requires leveraging it for meaningful use cases across the public and private sectors. A use-case or outcomes-driven approach ensures that DPI is not simply another piece of infrastructure, but a practical building block designed to deliver impact across various sectors. A focus on use cases can help reinforce the user-centricity needed to drive uptake and ensure that the infrastructure supports services that can improve people's lives. Specific use cases are also effective in mobilizing stakeholders—for example, partnering with financial service providers to design a use case for digital ID and data sharing can generate enthusiasm around the DPI project and spur later adoption.

The trade-off between sector-specific development and a DPI approach is a strategic decision that requires careful consideration of timing, coordination, and resource allocation. From a use case perspective such as delivering social assistance payments digitally, it is tempting to focus on sector-specific quick wins, which provide immediate results. However, this can lead to a patchwork of solutions that may be duplicative, expensive, with limited impact. The challenge often lies in the readiness of DPI to meet immediate sectoral needs, which can drive the momentum towards developing standalone infrastructures.

Sequencing the implementation of different DPIs and priority services is therefore critical and dependent on country context. Retrofitting existing systems, especially already digitalized services, to leverage DPI can be costly and challenging due to status quo bias. Existing country efforts to digitalize services should be considered when defining the initial priority use cases for DPI. For most use cases, multiple

49 For example, GovStack is launching "GovMarket" to identify providers with products that are compliant with GovStack specifications.

DPIs will play an important role, underlining the importance of interoperability between DPIs and across sectoral digital infrastructure. Coordination to develop and leverage DPI is time-intensive and at times politically challenging, but it lays the groundwork for long-term efficiencies and a platform for continuous innovation.

This section outlines some prominent DPI use cases, including for government-to-person transfers, financial inclusion, health, and agriculture. While these examples are illustrative, they are not exhaustive.

Government-to-Person (G2P) Payments

DPI is increasingly recognized as a driver transforming the delivery of G2P payments. G2P payments encompass all payments made by the government to individuals, including social assistance, pensions, public wages, and various subsidies. By providing shared and interoperable building blocks for digital transactions, DPI enables multiple government agencies to leverage the same infrastructure. This creates efficiency gains and helps government agencies avoid reinventing the digital wheel for each new payment stream or program.

DPI can help digitalize G2P payments in an efficient, inclusive, and adaptive way. When COVID-19 left billions of people in need of assistance, countries with elements of DPI in place were better able to reach the poorest in a faster, more targeted, and transparent manner. G2Px research on the role of digital during COVID-19 showed that among 85 countries, those that were able to use digital databases and trusted data sharing reached, on average three times more beneficiaries than

Box 7. DPI for social protection in Zambia

The Social Cash Transfer (SCT) is the Republic of Zambia's primary social protection initiative aimed at stabilizing the consumption of the poor. It involves small, frequent unconditional cash transfers, requiring payment points to be within 7 km of communities due to the difficulties beneficiaries face in traveling long distances. Prior to 2022, the program's management information system (MIS) was unstable, and all cash transfer payments were made manually in physical cash by civil servant Pay Point Managers (PPMs), most often teachers. This created challenges for accountability, payment reconciliation, and beneficiary authentication, increasing risks of error, fraud, and corruption.

The WBG supported the government of Zambia to overhaul this process by leveraging a payments gateway DPI and investing in a social protection MIS. For "urban areas" with network connectivity and payment service providers (PSPs) the government engaged multiple PSPs to reach a national scale, allowing beneficiaries the flexibility to select a PSPs of their choice, based on their knowledge of proximity of PSP locations. These payments are processed in real-time from the new CORE-MIS system and passed to the payment gateway. This facilitates a "double-entry" payments approach, where funds only leave the ministry's account if the balancing credit is successfully credited to each beneficiary account at the PSP. This means that in case of failed transactions there is no movement of funds and no need for the government to request refunds from the PSPs. For "rural areas" without network connectivity and PSPs, an Android mobile App was developed to record evidence of payments delivered in offline areas. Beneficiaries present their National Registration Card to ensure a match with the approved payroll downloaded from the MIS to the App.

The digitalization of payments has improved their timeliness and reduces duplicates and potential errors, fraud, and corruption. Leveraging the payments gateway DPI allows the government to maximize the integration effort with PSPs and reuse these for multiple other social protection programs. The MIS system and payment strategies have been adapted to support delivery to more than 2 million households, including almost 1 million as part of the ongoing emergency drought response. Evaluations show that when given the choice, beneficiaries tend to select the PSP with the closest, most convenient access point, reporting that this reduces travel expenses and frees up time to spend with family or on income-generating activities. Choice also gives the SCT program the flexibility to replace a PSP easily when one provider drops out or does not comply with the service standards. Allowing beneficiaries the choice of PSPs is therefore not only a more customer-centric approach but can also avoid reinforcing monopolies and protect program officers from being lobbied by PSPs.

Source: Adapted from World Bank (2021b) and World Bank (2022d).

those that could not rely on these DPIs and had to collect information from scratch (Marin & Palacios 2022).

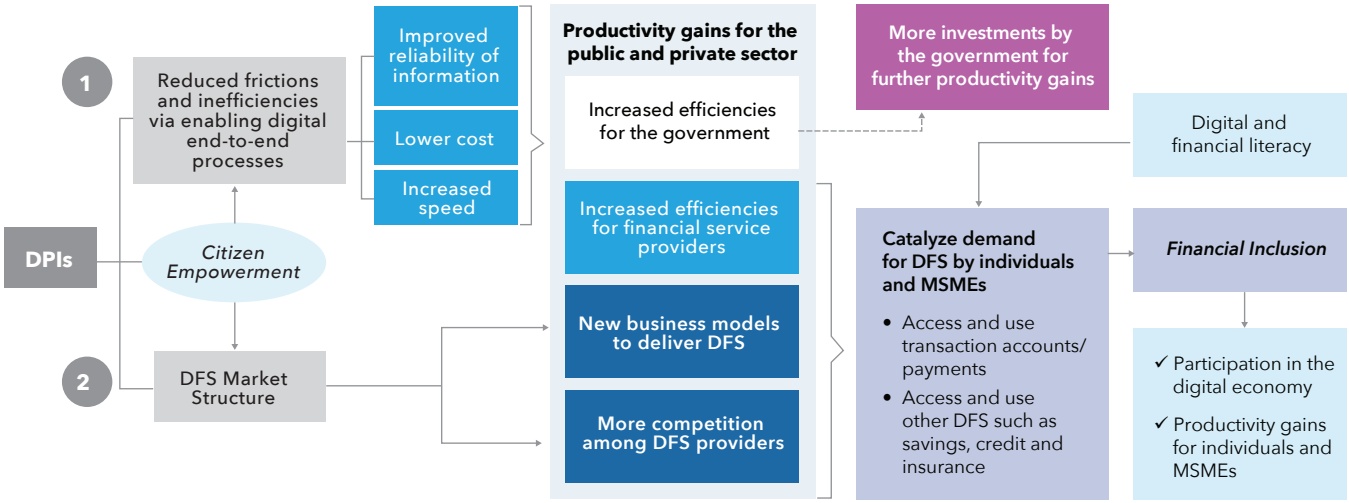
A modern G2P architecture[50] that utilizes DPI, particularly digital ID systems, payment clearing and settlement systems, and trusted data sharing frameworks, creates efficiencies and benefits for recipients and governments. Key processes in G2P payment delivery that benefit from DPI include account opening for payment recipients, registration with G2P programs, payment instructions, and fund transfers to financial institutions or treasuries, and the subsequent reconciliation and cash-out of digital transactions. An architecture leveraging DPI provides a unified digital platform for various G2P payment channels, resulting in fiscal savings for governments and fostering a payment ecosystem that enhances financial access and the development of relevant financial products and services, ultimately leading to increased convenience, inclusion, and empowerment for beneficiaries.

- Payment Systems that include both large volume and retail payment clearing and settlement systems, with wide participation from payment service providers and the availability of a government payment gateway or interface, are essential for the digital delivery of G2P payments. These payment systems can be used to direct payments into individual accounts, enabling governments to give payment recipients the choice of account and provider in which to receive their payments, thus unlocking further convenience and inclusion benefits.
- A trusted and inclusive ID system can support digital G2P payments, ensuring that beneficiaries have the necessary documentation to open financial accounts or can open an account remotely. In addition, a digital ID that provides services to sectoral systems (such as social registries and social protection MIS) can assist in identifying and enrolling potential beneficiaries into social assistance programs more easily.
- Aligned with a modern G2P architecture, DPIs can allow countries to offer beneficiaries a choice of payment service providers, which can increase convenience, promote financial inclusion, and contribute to market development. This requires an interoperable retail payment switch with broad participation from banks and non-bank payment service providers, along with a database or platform that supports the matching of beneficiary identifies and account numbers, known as an account directory. This allows beneficiaries to select and update their preferred account for receiving government payments without the need to coordinate with multiple programs or agencies.

Financial Inclusion

DPIs democratize financial access by enabling digital processes that reduce costs and extend the reach of financial services. DPIs democratize access by allowing financial institutions to leverage shared infrastructure, enabling broader reach and reducing operational expenses. The ability to verify identities and process applications digitally ensures that even remote

Figure 20. Role of DPI in financial inclusion



Source: Ardic Alper et al (2023)

50 See World Bank (2022c).

Box 8. Impact of PIX and digital G2P payments on financial inclusion

Since its launch in November 2020, the PIX fast payment system has significantly advanced financial inclusion in Brazil. The number of active users in the financial system more than doubled from June 2018 to December 2023, largely due to its contribution to the digitalization of financial services. The implementation of PIX, along with the distribution of emergency aid during the COVID-19 pandemic, played a crucial role in expanding access to financial services. Active clients of financial services increased from 77.2 million to 152 million, raising the proportion of adults with active accounts from 46.8 percent to 87.7 percent. The adoption of PIX has also benefited micro businesses, with the number of active business clients growing from 3.4 million to 11.6 million during the same period.

PIX has facilitated the expansion of financial service usage, particularly in digital credit and payment services. This led to a 3,000 percent increase in digital credit users. The cooperative banking sector also experienced substantial growth, especially in active credit users.

Source: Banco Central do Brasil (2023)

or economically marginalized communities can benefit from financial services.

Efficiencies and increased competition driven by DPIs play a crucial role in advancing financial inclusion. DPIs further productivity and financial inclusion through reduced inefficiencies and enhanced digital processes. By improving information reliability, lowering costs, and increasing speed, DPIs empower citizens and transform the digital financial services market, driving efficiencies for governments and service providers, fostering new business models, and enhancing competition. This, in turn, spurs demand for financial services among individuals and MSMEs, improving access to payments, savings, credit, and insurance. Together, these effects promote financial inclusion and productivity, enabling broader participation in the digital economy (Figure 20).

DPIs can improve the usage of financial services by making transactions more efficient, secure, and accessible. Payments DPIs, for example, allow for seamless and real-time transactions, which reduce the reliance on cash and make financial management more convenient for individuals and businesses alike. This efficiency encourages more frequent use of digital financial services and also builds trust in the formal financial system. In crisis situations, such as the COVID-19 pandemic, digital payments have proven invaluable, enabling governments to swiftly distribute financial aid, ensuring that even the most vulnerable populations receive timely support.

For MSMEs, digital payments provide critical tools that promote the effective use of financial services and support business growth. Digital payment platforms built as DPI enable MSMEs to track revenues, build credit histories, and access loans more easily. Additionally, data exchange infrastructures help financial providers use alternative data—like transaction records and utility payments—to assess creditworthiness, making formal financing options available to more businesses. This expanded access to credit supports entrepreneurship and stimulates economic development.

Advancing financial inclusion through DPIs requires a set of key enablers and catalyzers to maximize their value and support this objective. To achieve financial inclusion outcomes, several enablers and catalyzers are essential. DPIs add value by offering affordable identification, efficient payment solutions, and secure data exchange, which collectively lower barriers and make financial services more accessible. Strong governance and coordinated efforts are necessary to underpin DPI development, ensuring sustainability and a whole-of-society approach. Additionally, robust and widespread support services and infrastructure are critical for effective implementation, along with sound regulatory frameworks that provide clear, enforceable guidelines. Catalyzers such as widespread digital and financial literacy and inclusive financial service access points further promote financial inclusion.

Health

For health systems, DPI can serve as a catalyst to achieve the World Bank's goal of providing quality, affordable health services to 1.5 billion people by 2030. DPI that is effectively integrated into the health sector can play a critical role in advancing Universal Health Coverage (UHC) by lowering barriers to access healthcare services, enhancing efficiency, and improving health outcomes. Using elements of core DPI stacks makes digital systems in the health sector robust so

Box 9. Role of DPI in Indonesia's SatuSehat

Indonesia's SetuSehat program exemplifies a comprehensive approach to leveraging digital public infrastructure (DPI) for healthcare improvement. The program, launched in 2022, aims to create a robust, interoperable, and secure digital health ecosystem by integrating data from various technology-based apps and health facilities. At its core, SetuSehat relies on a standardized national health data system, which leverages a Master Patient Index validated by the Population and Civil Registration Agency (Dukcapil) to ensure accurate and secure digital identification. This digital ID system serves as the foundation for electronic medical records (EMRs) and facilitates seamless data sharing across the healthcare system.

Furthermore, SetuSehat integrates with the National Health Insurance scheme (JKN), administered by Badan Penyelenggara Jaminan Sosial-Kesehatan (BPJS-K). This integration enables secure and efficient electronic payments for healthcare services, streamlining the insurance claims process and reducing administrative burdens. The platform also facilitates data sharing between various stakeholders, including insurance companies, biotechnology laboratories, pharmacies, health-tech startups, and government agencies. This interoperability is achieved through open APIs based on microservices, allowing for secure and standardized data exchange across the ecosystem.

SetuSehat's success hinges on the establishment of a robust trust framework. The program prioritizes data protection and security, adhering to the Personal Data Protection Law passed in 2022. This legislation ensures data ownership rights, regulates data collection and usage, and imposes sanctions for data breaches. The program leverages a regulatory sandbox to test new digital health tools and associated legislation in a controlled environment, fostering innovation while mitigating risks. By utilizing digital ID systems, secure payments, data sharing platforms, and a strong trust framework, SetuSehat demonstrates the transformative potential of DPI in improving healthcare delivery and achieving universal health coverage in Indonesia.

they can fundamentally transform healthcare delivery, disease surveillance, and public health interventions. In the context of global health, data sharing can enable interoperable health information systems, digital identity frameworks can improve reliability of patient records, and digital payment interfaces can improve access to care and allow for more equitable healthcare financing. For healthcare financing and access, fast payment systems create opportunities for integrated payment infrastructure within health systems that can streamline insurance claims, government health scheme payments, and out-of-pocket expenses. Trust-based digital authentication systems can also combat counterfeit medicines by enabling verification at every step of the supply chain.

Utilizing DPI in the health sector requires careful consideration of privacy protections, human capacity, and interoperability challenges. Health data demands exceptional privacy protections and security measures while simultaneously needing to be accessible across different healthcare providers (both public and private) and jurisdictions, and in some cases support cross-border data exchange, enabling early warning systems for disease outbreaks and coordinated international responses to health emergencies. Countries must also invest in building the human capacity to maintain and evolve these systems, as health technologies and standards continuously advance. The COVID-19 pandemic demonstrated how countries with an established digital health infrastructure were better positioned to implement contact tracing, vaccine distribution, and telemedicine services, highlighting the critical need for such systems to be developed as public goods rather than proprietary solutions.

Agriculture

The agriculture sector is a prime use-case for DPI, with the potential for large-scale transformational impact. Globally, approximately 1 billion people (ILO 2024, via World Bank DataBank) and two-thirds of the world's poorest are engaged in or depend on agriculture for their livelihoods (UN 2023). DPI enables a technology and data-driven approach to agriculture based on interoperable systems, dynamic digital infrastructure (particularly digital ID, e-payments and e-signature systems), data-sharing mechanisms, and a robust trust ecosystem. By leveraging foundational components, DPI can foster efficient

and transparent transactions in the agriculture sector that empower farmers, governments, and agribusinesses alike by facilitating timely access to information, financial services, and Digital Public Goods (DPGs). Overall, DPI offers a scalable solution to address key challenges such as:

- **Access to Services:** Improved digital IDs and digital payments can enhance access to critical services such as input subsidies, agricultural credit, crop insurance, and real-time advisory services—key tools for mitigating risks and improving productivity and income.
- **Data-Driven Timely Decision-Making:** Interoperable systems and data-sharing capabilities allow policymakers and agribusinesses to make informed decisions based on additional data such as on crop patterns, land use, and environmental data.
- **Climate Resilience:** The agriculture sector is particularly vulnerable to climate change (Mbow et al. 2019). Here, DPI can be leveraged for both adaptation and mitigation measures. For example, DPI can support sector-specific digitalization efforts, such as farmer and farm IDs, to enhance adaptation and mitigation efforts through government benefits and tools like real-time weather advisories and region-specific climate-smart inputs.
- **Efficient Markets:** Digital payment systems and data sharing capabilities can support online marketplaces that can reduce transaction costs and expand market access.
- **Inclusivity:** DPI in agriculture can promote inclusivity, especially for smallholder farmers who often lack access to essential financial and information services. DPI can bring marginalized rural populations into formal economic systems, enabling them to access credit, make digital payments, and secure insurance and other services.
- **Agribusiness models:** As food security becomes more pressing, there is a need to enhance agribusiness models. DPI can be leveraged to improve the efficiency, transparency and resilience of food systems, enabling monitoring of production, storage and distribution. For example, farm and farmer IDs, based on official digital

Box 10. India's AgriStack

India's AgriStack exemplifies how DPI can revolutionize agriculture at scale. India's AgriStack, an initiative by the Government of India is built on the country's foundational DPI. It serves as an example of how sector-specific solutions can be built upon existing core DPI. Specifically, AgriStack's leveraging of Aadhaar (the national digital ID system) for farmer identification demonstrates exactly how foundational DPI can enable digital transformation across sectors without reinventing core infrastructure.

The AgriStack aims to create a unified digital ecosystem for the agricultural sector by integrating multiple data streams, including farmer identities, land records, and crop information. At its core is a digital farmer's registry, which provides each farmer with a unique digital ID, built on the Aadhaar system, enabling them to access government schemes and benefits more easily. Further, agriculture benefits (such as farm subsidies, crop insurance, credit, etc.) in India are often received directly into Aadhaar-linked bank accounts of eligible farmers and require Aadhaar numbers to receive benefits to reduce administration, targeting and fraud related costs.

India's AgriStack has built other databases which leverage the farmer and in-turn Aadhaar registry such as the geo-referenced village database and the crop sown registry. These databases link each farmer's identity with their land records and crop details, allowing for a comprehensive view of agricultural activities across the country.

Through the AgriStack, the government can better monitor crop patterns, allocate resources, and deliver targeted services such as crop insurance and subsidies. It also enables digital crop surveys each season, providing critical data to enhance productivity, manage risk, and support policy planning. By leveraging mobile-based platforms (WEF 2023), AgriStack makes it easier to conduct on-the-ground data collection, making the system more responsive and adaptable. This initiative has potential not only to support individual farmers but also to create a foundation for a robust agri-tech ecosystem (Beriya 2022) in India. AgriStack is a pioneering example of how DPI can be leveraged to enable efficient, data-driven, and inclusive agricultural policies that benefit farmers and stakeholders alike. For more information see https://agristack.gov.in/

IDs, can be linked to platforms that track crop health to help farmers make more informed decisions. Similarly, IoT-based sensors in warehouses and distribution networks can be linked to other datasets based on data sharing standards or through data sharing platforms to ensure monitoring of the storage and transportation of food.

To scale and leverage DPI for agriculture globally, significant and coordinated investments are needed. These investments include in foundational DPI, overall digital ecosystem (such as connectivity, digital skills, advanced data processing capabilities, and cloud computing) and agriculture-specific digital systems (such as digitalization of agriculture services, farm and farmer registries, agriculture platforms) are necessary. Lessons from initiatives like **Kenya's** Big Data Platform (Box 2) and **India's** AgriStack (Box 10) also demonstrate the importance of DPI systems such as system interoperability, standardized data-sharing protocols, and governance frameworks that protect farmer privacy while enabling efficient data utilization.

Long-term coordinated financial commitments are required, and investments should prioritize interoperability and connectedness to ensure equitable access. Capacity building is also essential to empower local experts and farmers with the knowledge and tools to effectively leverage DPI-enabled services. Investments should support training programs, digital literacy campaigns that would be beneficial across sectors as well as, with the agriculture-sector, farmer-centric platforms, including registries, payment systems, and advisory tools, to ensure user-friendly and inclusive access.

IV KEY LESSONS

As Section 3 demonstrated, there is no single blueprint for designing and implementing DPI. The type of DPI system, country context, and use cases matter. However, it is still possible to identify some high-level good practices and principles around DPI and its use. This section synthesizes some of these lessons, highlighting five success factors to help harness the potential of DPI while mitigating key challenges and risks and providing concrete examples that can be incorporated into policy and project design.

These lessons build on existing guidance on broader digitalization efforts and on implementing specific systems as DPI. For example, the Principles for Digital Development[51] provide a high-level set of guideposts for rolling out any digital system or strategy that resonate strongly with the DPI approach, including the importance of sharing and reuse, designing with people and for inclusion, creating open and transparent practices, and mitigating potential harms. For digital identity systems in particular, the Principles on Identification for Sustainable Development[52] establish 10 principles for inclusive and trusted ID systems, focusing on universal access, design principles around interoperability, security, and privacy-by-design, and comprehensive governance and oversight.

1. SAFETY AND INCLUSION FIRST

The success of DPI hinges on its ability to deliver safe and inclusive digital services that benefit all members of society. This requires a fundamental shift in how the world approaches digitalization, moving beyond technology to creating a trusted and accessible ecosystem. Some key success factors include:

- **Legal and regulatory reforms:** Laws and regulations are critical for ensuring that DPIs are safe and inclusive, providing a trusted environment for digital services. A comprehensive approach to legal and regulatory reforms is often necessary to address the broad spectrum of safety and inclusion within DPIs. However, by prioritizing legal reforms essential to core DPIs (such as digital ID, e-signatures, digital payments, and data-sharing) and then expanding to more sector-specific regulations, countries can help lay the foundations for a safe and inclusive digital infrastructure that can gradually be expanded and refined as the surrounding ecosystem matures. In **Jordan**, the prioritization of strategic reforms was key to advancing DPI, a strategic commitment for the country since 2021. Notable reforms such as the recognition of electronic transactions and e-signatures, a revised law on access to information, the adoption of a law against cybercrime, and the new data protection law. While additional reforms are still needed to address all aspects comprehensively, these foundational changes have enabled Jordan to make substantial progress in deploying DPI safely and inclusively.
- **Security- and rights-enhancing:** DPIs must be built with robust data protection and security measures in their DNA. Data breaches and misuse can erode public trust and undermine the very benefits DPI aims to deliver. In addition to a strong legal and regulatory framework, countries should prioritize privacy-enhancing technologies and continuous investment in cybersecurity. Data privacy and human rights impact assessments throughout the DPI development process are crucial. This involves conducting thorough assessments to identify potential risks and implementing mitigation measures to address them. In **Australia**, for example, the Commission Report on Data Availability and Use that preceded the Consumer Data Right framework (a data sharing DPI), included multiple rounds of consultation and privacy impact assessments (Desai et al. 2022).

51 See https://digitalprinciples.org/.
52 See http://idprinciples.org.

- **Accessible design:** DPIs, as well as any service and product built leveraging DPI, should be universally accessible, accommodating diverse needs and ensuring no one is left behind. This includes incorporating universal accessibility features to cater to individuals with disabilities, simplifying user interfaces for those with limited digital literacy, and offering alternative non-digital options for those who prefer them. Proactive outreach and testing with marginalized groups are essential to identify and address potential barriers to adoption, as done in **Indonesia** (see Section 3).
- **CSO engagement:** Engaging with civil society organizations (CSOs) throughout the process is vital to ensure diverse perspectives are considered and to build trust in the DPI ecosystem. For example, **Jordan**'s open government data initiative, which involved extensive public consultations with CSOs, has fostered a more transparent and accountable data sharing environment (see section 3).

2. FOCUS ON OUTCOMES, NOT TECHNOLOGY

Avoid thinking of DPI as a new technology that will save the day; instead, focus on outcomes and use cases, and work backwards to arrive at priority investments, architecture, and technology choices. It is essential to prioritize the outcomes and practical applications over the allure of new technology. The goal is not to find a technological panacea but to identify and invest in solutions that address specific needs and deliver tangible benefits. This outcome-driven approach requires a careful analysis of the desired impact, and a strategic selection of technology based on those goals.

- **Use case assessments are a critical starting point.** By thoroughly understanding existing challenges in service delivery and digital transactions, stakeholders can identify use cases where DPI is likely to have a large impact (and where it is not the most pressing issue). This understanding should guide the design and implementation of DPIs, ensuring that technology choices are fit for purposes—such as improving the efficiency of social protection programs, enhancing financial inclusion, or streamlining e-services. These assessments should be informed by a country's unique constraints and a clear vision of the intended users and their needs. In 2023, for example, the World Bank partnered with the government of **Lebanon** to conduct a use case analysis, identifying where and how integrating digital identity within a broader digital transformation program could enhance the delivery of public services in the country (World Bank 2024b).
- **Stakeholder consultations are vital in this process.** Engaging with the diverse array of users—from individuals and businesses to government entities—ensures that DPI meets real-world demands and is user-centric. This collaborative approach helps to identify the most pressing issues and fosters a sense of ownership and alignment among all parties involved. In 2020, **South Africa** launched a series of community consultations as part of an effort to reform its national identity system to be more inclusive. Consultations revealed that the gender-coded identification number in the national ID system excluded nonbinary and transgender individuals, prompting regulatory changes (DHA 2020). In **Jamaica**, a CSO coalition successfully reviewed the new ID legislation, achieving consensus on various provisions and actively participating in the legislative process, with their contributions publicly acknowledged by the government.[53]
- **An outcomes-based strategy also requires data and research.** To maximize the potential of DPI and keep the focus on outcomes, rigorous evidence-building is needed to test and document impact. Measuring impact cannot be an afterthought; rather, strategies for assessing and calibrating effectiveness should be built into the design and rollout of DPIs. This entails developing clear, actionable metrics and research designs (including robust impact evaluations) to evaluate not only the tangible benefits—such as efficiency gains or service reach—but also the quality of citizen experiences, including their satisfaction, trust, and sense of inclusion. The World Bank is supporting this type of work through the launch of DPI-specific research labs, including in **Ethiopia**, **Philippine**s, and **India**.[54]
- **Feedback loops and participatory evaluations are also essential to ensure that DPIs evolve in response to user needs and maintain public confidence.** For example, tracking adoption rates alongside qualitative measures of citizen satisfaction can illuminate the reasons behind

53 For more information about the CSO coalition in Jamaica, see: https://nidsfocus.com/.

54 DPI research labs are a collaboration between the World Bank's ID4D, G2Px, and Development Impact Evaluation (DIME) programs, country governments and DPI providers and users, and multiple academic research partners and donors. The goal is to outline priority research topics around specific DPI implementations and mobilize a research and partnership community to support and execute these studies. For more, see ID4D and G2Px's most recent Annual Report (World Bank 2024c).

success or stagnation. By grounding DPI initiatives in robust evidence and meaningful engagement, stakeholders can build infrastructures that are both technically sound and deeply aligned with the needs of the people they serve. The varied uptake of DPIs, illustrates that widespread adoption requires clear value propositions, widespread availability, and trusted processes. For example, **Australia**'s Consumer Data Right (CDR)[55]—an opt-in data sharing service—outlines key use cases for data sharing, benefits for individuals, and its overall vision for the customer journey (Desai et al. 2022).

3. USERS AT THE CENTER

Countries should create DPIs—and DPI-enabled services—that are tailored to the needs, behaviors, and experiences of users. By integrating "service design" and human-centric design (HCD) principles into the development of DPI, governments and organizations can create more effective, efficient, and user-friendly services that are more likely to be adopted and valued by the public. Implementing these approaches can involve the following:

- **User Research:** Conducting in-depth research to understand the needs, pain points, and behaviors of the end-users. This can include interviews, surveys, field studies, and usability testing. User journey mapping can be a particularly useful tool to visualize the steps users take when interacting with a DPI service. This includes identifying pain points, frustrations, and areas for improvement. For example, ID4D has worked with governments in **Ethiopia**, **Nigeria**, **Rwanda**, **Indonesia**, **Philippines**, **Timor Leste**, and others on qualitative research studies to inform the design of digital ID systems.[56]
- **Co-Creation:** Involving stakeholders, including end-users, in the design process to ensure that the solutions developed are aligned with their needs and expectations. Workshops and collaborative design sessions can be effective in this stage. Incorporating digital citizen engagement through participatory design mechanisms such as crowdsourcing platforms and public consultations, can offer valuable insights on ensuring DPIs effectively meet user needs.
- **Prototyping and Testing:** Developing prototypes of the DPI user interfaces or DPI-enabled services and testing them with real users to gather feedback. This iterative process helps refine the solutions to better meet user needs. In a series of blog posts, **Singapore**'s National Digital Identity program detailed how they revised their ID system to better meet individual needs, including conducting "real life" testing to identify unexpected challenges users faced while using their mobile app.[57]
- **Service Blueprinting:** Mapping out the service interactions across different touchpoints and channels to ensure a seamless user experience. This helps in identifying any gaps or areas for improvement in service delivery.
- **Accessibility and Inclusivity:** Assessing that the DPI is accessible to all users, including those with disabilities, and designing for inclusivity to cater to the diverse needs of the population. For example, **Indonesia** has engaged in significant user testing with women, persons with disabilities, and low literacy groups for its new digital ID app.
- **Iterative Design:** Continuously improving the service based on user feedback and changing needs. This agile approach allows for adjustments to be made as new insights are gained.

Ideally, the above approaches can be designed and managed by staff dedicated to user experience. For example, the **UK** Government Digital Service employed various techniques like assigning a dedicated researcher to each project team, using an experimental design approach, and regularly observing end users interacting with their products to make their services more aligned with people's needs.[58] The **Italian** Digital Agency developed a comprehensive manual for the Public Administration's websites and digital services, offering operational guidance on topics such as digital administration design, project management, service design, user experience, accessibility, and interface design.[59]

55 For more, see https://www.cdr.gov.au/.

56 Reports from many of these studies are available on the ID4D website at https://id4d.worldbank.org/research. ID4D's Qualitative Research Toolkit (Bailur & Esquivel Korsiak 2019) also provides additional guidance on conducting this type of study, and is available at https://id4d.worldbank.org/qualitative-research.

57 For more information about how the Singaporean GovTech agency is performing user research to improve their ID system and processes, see their series of blogs at https://medium.com/ndi-sg/making-digital-services-more-accessible-for-all-part-1-a150ef027ea4

58 For more information about the way GDS team applied user research to their activities, see Gov.UK Blog at https://gds.blog.gov.uk/2013/08/30/how-we-do-user-research-in-agile-teams/.

59 For more information, see the "Manuale operativo di design" (Operational Design Manual) at https://docs.italia.it/italia/designers-italia/manuale-operativo-design-docs/it/versione-corrente/index.html.

4. INVEST IN PEOPLE

Investing in human capital is a cornerstone of successful DPI deployments. This investment transcends mere technology acquisition; it is about empowering individual stakeholders—civil servants, businesses, and individual users—to navigate and leverage DPI and DPI-enabled services effectively. This investment is the bedrock upon which the success of DPI initiatives is built, ensuring they are inclusive, sustainable, and resilient in the face of rapid technological change.

For the government, training and capacity building for public servants to be able to develop, regulate, supervise or leverage DPI is paramount. Incentives are also crucial for attracting and retaining the qualified personnel necessary to operate and innovate within the DPI ecosystem. For example, **Singapore**'s approach to revamping compensation packages for data talent and creating specialist career pathways attracts and retains high-caliber professionals, while **Mauritius**' National Open Data Policy, which mandates the creation of Open Data teams within each ministry, illustrates the importance of structured capacity building at various government levels (Desai et al. 2022). In **Colombia**, the government published a profile for chief data officers that helps define core competencies required in this role across public sector agencies, laying the groundwork for advanced skills building (World Bank & IADB 2024).

Digital literacy for the population at large is another critical investment. A digitally literate population can better leverage the opportunities DPI unlocks while minimizing exclusion risks, ensuring that the benefits of digital services are widely accessible. Initiatives like **Estonia**'s "Tiger Leap," which invested massively in connectivity and digital skills, and **Singapore**'s Digital Readiness Blueprint, which had the goal of ensuring that all Singaporeans have access to technology to improve their lives, have been instrumental in fostering a digitally savvy citizenry (Desai et al. 2022). **Uruguay** has similarly promoted "digital citizenship," including the development of a set of basic digital skills to enable access, retrieval, understanding, evaluation (Desai et al. 2022).

5. IT TAKES A VILLAGE TO BUILD GOOD DPI

A whole-of-society—and cross-border—approach is important for building and sustaining DPI and other ecosystem components. Each country will have a unique set of key stakeholders and respective roles they can play. While this broad ecosystem can create complexities for coordination, it also creates opportunities for multiple agencies to make progress on building or using DPI simultaneously. Importantly, this requires building strong institutions and champions for DPI not only in the central government and digital ministries or agencies, but across other sectors and ministries, and with the private sector. International collaboration is essential for encouraging interoperability and open and common standards to enable digitalization of cross-border services and transactions.

Example roles and opportunities across stakeholders include:

Public Sector:

- Lead the development of a national, cross-sector DPI strategy in cooperation with the private sector, ensuring alignment with broader digital transformation goals.
- Establish policies to ensure the long-term sustainability of DPI initiatives, such as through securing public resources to fund government-built DPI and crowding in private sector investment.
- Develop a legal and regulatory framework that supports DPI development and adoption, including data sharing, privacy, and cybersecurity policies, as well as sector- and DPI-specific relevant regulations.
- Foster collaboration across public and private sectors to ensure seamless integration, interoperability, and service delivery.
- Establish and promote technical standards for data sharing, verifiable credentials, and digital services to ensure consistency across sectors.
- Create enabling environments for innovation, such as regulatory sandboxes, to test and iterate on digital solutions.
- Safeguard consumer rights, promote awareness, and ensure access to grievance mechanisms within the DPI ecosystem.
- Build DPIs (as needed, or as defined by national strategy), potentially in collaboration with the private sector.

Private Sector and Start-ups:

- Build DPIs, potentially in collaboration with or as regulated by government.
- Integrate DPIs into existing digital services.
- Innovate on top of DPI platforms to create value-added services.
- Promote trust in DPI by providing audit, conformity assessment, cybersecurity, and other services.
- Partner with the public sector to drive technology adoption and digital literacy.
- Contribute to the development of open standards and interoperable solutions.
- Develop new DPI technologies, services, and solutions.

Civil Society and Non-Governmental Organizations:

- Advocate for inclusive and equitable DPI that serves all segments of society, with a focus on at-risk or marginalized groups.
- Participate in policy discussions and provide feedback on DPI initiatives to ensure that design responds to user needs and minimizes exclusion and other risks.
- Participate in established DPI governance bodies, such as public oversight committees.
- Engage in community monitoring and capacity building to improve implementation and accountability for DPI and its use.
- Help to build and support open standards and digital public goods for DPI.
- Support digital literacy and awareness campaigns to empower citizens.

Academics and Researchers:

- Partner with DPI ecosystem members to conduct novel research and data collection to improve and measure DPI impact.
- Propose evidence-based policy recommendations for DPI providers based on new research.
- Develop and test new DPI technologies, services, and solutions.

International and Regional Bodies:

- Facilitate cross-border collaboration and standard-setting for DPI, including adopting frameworks for interoperability and recognition of digital identity, e-signatures, and transactions, as well as cross-border payments and data sharing.
- Share best practices and provide platforms for knowledge exchange.
- Support capacity-building in developing countries for DPI implementation.
- Help build and support open standards and digital public goods for DPI.

Standards Development Organizations:

- Develop and maintain technical standards for components of DPI.
- Promote interoperability across digital systems by creating standardized frameworks that facilitate cross-platform and cross-border integration.
- Engage with stakeholders to ensure that standards remain relevant given technological advances.

Accreditation Bodies:

- Accredit auditors that assess the technical and operational compliance of DPI systems.
- Promote accreditation of actors that ensure trust in DPI such as certification bodies and testing laboratories.
- Facilitate cross-border recognition of accredited services and certifications.

By embracing a whole-of-society approach and public-private partnerships, stakeholders can overcome inertia and legacy constraints. This shift in mindset requires high-level political champions and a well-coordinated strategy to ensure buy-in and mobilization among all stakeholders. Center-led initiatives are likely to be insufficient, and complementary sector-led digitalization efforts can help boost momentum and uptake of DPI. Robust and resourced institutions are essential for enforcing rules and offering effective redress. Iterative policy environments and agile institutions will enable continuous learning and improvement, adapting to the fast-paced evolution of technology and data governance.

A well-designed DPI may have the ability to unlock shared cross-border growth. For example, the adoption of **Estonia's** X-Road by several countries facilitates cross-border data exchange and economic linkages. Cross-border collaboration for DPIs is also essential. For example, FPS interlinking enhances the end-user experience in cross-border payments by providing 24/7 availability, improving transaction speed, reducing costs, and ensuring greater transparency through standardized messaging, modern technology, and a common rulebook. However, this progress comes with multiple challenges. To address these, stakeholders in multi-jurisdictional contexts should establish clear legal, ownership, and operational structures while leveraging international standards.

Box 11. The role of different public sector stakeholders in a country's DPI journey

The relevant government stakeholders and the specific roles each might plan in DPI will vary across countries. Below is a sample list of potential roles different public stakeholders could have.

Digital Government Authority or Similar:

- Lead or champion DPI, ensuring alignment with national digital strategies.
- Foster innovation for digital services and data sharing across sectors.
- Coordinate with other government entities and the private sector to ensure interoperability and seamless service delivery.
- Publish an optional standard for verifiable credentials to encourage ministries, departments, and various levels of government to issue their certificates and documentation digitally.
- Encourage line ministries and departments to provide open APIs for their online services to enhance user experience and service delivery.
- Lead or champion efforts to revise or create laws to enable e-signatures and digital transactions, as well as the implementation of trust frameworks and standards for digital identity and e-signatures.
- Potentially lead the development of online digital ID and data sharing systems (can also be done by ID agency and/or private sector, based on context).

Ministry of Finance:

- Secure funding for DPI initiatives and ensure financial sustainability of government-built DPIs.
- Work with other ministries to align budgeting with digital transformation goals.
- Implement financial policies that incentivize digital adoption, innovation, and private capital mobilization for DPIs.
- Integrate DPIs into public financial management systems as appropriate.

Central Bank and Financial Regulators:

- Foster an enabling digital financial ecosystem.
- Support or lead the development of fast payments systems.
- Develop an eKYC/CDD policy to facilitate DPI adoption.
- Develop a regulatory framework for Open Finance, including technical specifications for financial data sharing across sectors.
- Develop and enforce financial sector specific regulatory and supervisory frameworks for financial sector cybersecurity, data protection, consumer protection, and other safeguards.

Digital Regulators and Accreditation Bodies:

- Review and reform legacy legal frameworks to eliminate barriers to DPI adoption.
- Create regulatory sandboxes to allow for testing and iteration of digital solutions.
- Lead or champion efforts to revise or create laws to enable e-signatures and digital transactions, as well as the implementation of trust frameworks and standards for digital identity and e-signatures.
- Develop certification and qualification schemes for digital ID and trust service providers.

Consumer Protection Authorities:

- Enforce compliance with national consumer protection laws and regulations across the DPI ecosystem.
- Promote consumer rights, educate, and raise awareness of the various stakeholders involved in DPI.
- Facilitate complaint mechanisms and dispute resolution arising from the use of DPI-enabled services.
- Advocate for consumer interests in policy development related to DPI.

Data Protection Authorities:

- Enforce DPI compliance with data protection laws and regulations.
- Develop and publish guidelines to strengthen the normative framework for data protection.
- Oversee data practices within the DPI ecosystem, investigate and address violations.
- Promote awareness of public and private sector organizations involved in DPI about data protection best practices and inform data subjects about their rights and mechanisms to enforce them.
- Oversee and resolve complaints lodged by data subjects including breaches and other violations of their individual rights.
- Coordinate with relevant national and cross-border agencies to ensure a holistic approach to safeguarding data within the DPI ecosystem.

Cybersecurity Authorities:

- Set national or regional cybersecurity policies that protect and ensure trust in DPI.
- Offer guidance and certification schemes to ensure that DPIs meet cybersecurity standards and can withstand emerging threats.
- Coordinate response to cybersecurity incidents that impact DPI, ensuring quick recovery and continuity of services.

ID and Civil Registration Authorities:

- Implement foundational ID and civil registration systems as trusted sources of legal identity and vital records (e.g., birth, marriage, divorce, death).
- Ensure universal access to ID and civil registration coverage among the population.
- Add capabilities to existing ID and civil registration systems to operate as DPIs (e.g., opening up systems to allow third parties to verify data and credentials)
- Potentially lead the development of online digital ID systems (can also be done by digital agency or private sector based on context).

Line Ministries:

- Integrate DPI into sector-specific strategies and service delivery models.
- Build new sector digital infrastructure following a DPI approach (modular, interoperable, etc.) so that it can easily integrate with existing or future DPI).
- Collaborate with DPI providers to ensure sectoral needs are met.
- Review laws and regulations for digital readiness and data sharing.
- Engage in capacity building to leverage DPI for improved service outcomes.
- Develop core registers using common data formats and interoperability standards.

V FORWARD LOOK

This paper outlines a framework for understanding and supporting the development of DPI as a driver of inclusive and transformative development. Despite this potential, the successful implementation of DPIs requires a concerted effort across government, the private sector, civil society, and the global community. Each country's DPI and digitalization journey will be unique; however, there are some common considerations and lessons. This paper has provided insights into these emerging good practices and also uncovered areas where further research and guidance will be needed.

The WBG's Global DPI Program is a new cross-sectoral and multi-donor initiative to support countries in building safe, inclusive, and transformational DPI. The program will build on the successes of the existing ID4D and G2Px Initiatives, and other efforts including Project FASTT, expanding in scope to cover data sharing and additional use cases. It will bring together teams across the WBG—including those working on agriculture, digital transformation, financial inclusion, gender, governance, health, legal, private sector investment, research and data, social inclusion, and social protection—to harness multisector expertise and financing to support DPI and its use.

The DPI Program will focus on developing policy-relevant data and guidance, supporting country and regional clients, and engaging in global advocacy around practical strategy questions. It will also support the design and implementation of next-generation DPI in line with good practices, including diagnostics and assessments, technical assistance, capacity building, and peer exchange. Priority areas for the WBG to bridge some of the knowledge gaps outlined in this paper under the Global DPI Program will include:

Strengthening DPI Strategy

- **DPI diagnostics and maturity models:** Developing diagnostics and maturity models to assess the status quo of DPI ecosystems across countries and identify areas for investment. This could involve developing tools to assess core DPI systems, as well as the broader policy, technology, and capacity needed to build safe and inclusive DPIs across a variety of contexts, including for low-income and fragile, conflict-affected, and vulnerable countries.
- **Building DPI champions and capacity:** Providing knowledge, training, and peer-exchange resources and support to help build in-country capacity related to DPI, including fostering multi-stakeholder alignment and collaboration across the public and private sector and with civil society.
- **Strategies for sequencing and change management:** Exploring optimal approaches to the timing and integration of DPI components relative to sector-specific systems and services, including whether DPIs should be established first or if sectoral use cases can be developed concurrently and later integrated, and how to effectively manage change by overcoming institutional inertia and vested interests.

Implementing Safe and Inclusive DPI

- **DPI legal and regulatory reforms:** Supporting legal and regulatory reforms to ensure that DPI systems are implemented in a safe, inclusive, and sustainable manner. This could involve providing DPI-specific guidance on data privacy and protection, cybersecurity, and public engagement to minimize risks to data privacy and exclusion.
- **Data sharing and governance frameworks and models:** Developing guidance and frameworks for data sharing, including definitions, types, models, and operationalization, including those that are appropriate for different use cases (open data, public intent data, personal data, and more), and different contexts (for example, low connectivity or low-trust environments).
- **Decentralized solutions for digital identity and data sharing in developing countries:** Developing guidance and support for the development of decentralized solutions for digital identity and data sharing, particularly in

developing countries. This includes a focus on wallet/VC implementations, including architectures that work in online and offline environments and cases where smartphone penetration is low.

- **DPI procurement, architecture, and financing:** Developing guidance on procurement processes, systems architecture, and financing options for DPI, with a focus on understanding how different strategies (including the use of DPGs) impact overall costs, capacity requirements, time-to-deploy, sustainability, and potential for lock-in. This will involve exploring existing procurement and architecture models, identifying market and financing gaps, and building capacity to manage procurement and contracts effectively.
- **New forms of DPI:** As countries advance in their digitalization agendas and the concept of DPI matures, additional types of core DPI may emerge. For example, some have argued for an additional category of DPI focused on enhancing the discoverability of services and providers (such as through open protocols and APIs) to improve public service delivery and enhance peer-to-peer transactions, such as the Beckn Protocol (CDPI 2024b). The World Bank will follow these developments and incorporate additional guidance on new DPIs as needed.

Adopting DPI for High-Impact Services

- **Sector roadmap for use case integration and sequencing:** Developing guidance on how to integrate DPI into specific sectors (such as financial services, social protection, health, agriculture, and public financial management), including sequencing and retrofitting DPI systems in relation to sector-specific systems and services, required regulatory reforms by sector, questions on interoperability and data standards, and more.
- **Core government registries as foundations of DPI:** Exploring whether and how existing core government registries (such as for birth, death, marriage, land, business) might be leveraged as foundational elements of data sharing and other DPI. This will involve examining how to improve data quality, interoperability, and accessibility of these registries to support broader digital service delivery.
- **Data collection and research on DPI:** Building the evidence through advanced data collection and research, with a focus on measuring DPI gaps and progress, identifying successful strategies for implementation, and estimating the impact of DPI for people, governments, and businesses.

By combining financial resources with a strong knowledge agenda and partnerships, the WBG and other development partners can help countries accelerate their digitalization through a DPI approach. While this paper has spelled out some core lessons and success factors, each country will chart a unique digitalization journey based on their starting point, available resources, and desired objectives. This will require dedicated champions in the public and private sector to build, operate, and govern DPI systems , and to invest in broader digitalization across government and the economy. Through the Global DPI program, the WBG will continue to support countries holistically on these journeys, including through thought leadership, research, global convening, technical assistance, and financial support to build safe and inclusive DPI under the Digital GCP and IDA21.

REFERENCES

Alberto Di Iorio, Anneke Kosse, and Robert Szemere. 2024. "CPMI Brief No 3: Tap, click and pay: how digital payments seize the day". February 2024. Bank for International Settlements' Committee on Payments and Market Infrastructures (CPMI). Available at https://www.bis.org/statistics/payment_stats/commentary2402.pdf.

Ardic Alper, O.P., Galicia Rabadan, G.A., Marin, G., Natarajan, H., Piveteau, T.Y., Ramteke, N.C., and Sarkar, A. 2023. "G20 Policy Recommendations for Advancing Financial Inclusion and Productivity Gains through Digital Public Infrastructure." Washington, D.C.: World Bank Group. http://documents.worldbank.org/curated/en/099092023121016458/P178703046f82d07c0bbc60b5e474ea7841.

Bailur, S. and Esquivel Korsiak, V. 2019. *Understanding People's Experiences with Identification: A Guide for Qualitative End-User Research on ID*. Washington, DC: World Bank Group. http://documents.worldbank.org/curated/en/795541561701481546/Understanding-People-s-Experiences-with-Identification-A-Guide-for-Qualitative-End-User-Research-on-ID

Banco Central do Brasil. 2023. "Relatório de Economia Bancária" https://www.bcb.gov.br/content/publicacoes/relatorioeconomiabancaria/reb2023p.pdf

Bank of Thailand. 2024. "PS_PT_018 Use of PromptPay 1/." Accessed on 19 August 2024 at https://app.bot.or.th/BTWS_STAT/statistics/BOTWEBSTAT.aspx?reportID=921&language=ENG.

Beriya, A. 2022. "India Digital Ecosystem of Agriculture and Agristack: An Initial Assessment." ICT India Working Paper #68. https://csd.columbia.edu/sites/default/files/content/docs/ICT%20India/Papers/ICT_India_Working_Paper_68.pdf

Casher, C., Metz, A., and Clark, J. 2024. "ID4D Global Dataset 2021: Volume 3 - Trends in Identification for Development." Washington, DC: World Bank. https://documents.worldbank.org/en/publication/documents-reports/documentdetail/099031924132035631/p17634114229a80dc18ea11c4c279817517?_gl=1*123id7t*_gcl_au*MTczNDYzMzQ0NS4xNzIyMDAyMzc5.

Centre for DPI. 2024a. "Is my system a DPI?" DPI Wiki. Retrieved from https://docs.cdpi.dev/.

Centre for DPI. 2024b. "Discovery & Fulfilment." DPI Wiki. Retrieved from https://docs.cdpi.dev/.

Centre for DPI. 2024c. "Identifiers & Registries." DPI Wiki. Retrieved from https://docs.cdpi.dev/.

Centre for DPI. 2024c. "eConsent." DPI Wiki. Retrieved from https://docs.cdpi.dev/.

Chowdhury, A. 2024. "Bangladesh's "phygital public infrastructure" bridges DPI theory and practice." GovInsider Asia, 5 October 2024. https://govinsider.asia/intl-en/article/bangladeshs-phygital-public-infrastructure-bridges-dpi-theory-and-practice.

Clark, J., Metz, A., and Casher, C. 2022. ID4D Global Dataset 2021: Volume 1 - Global ID Coverage Estimates. Washington, D.C.: World Bank Group. http://documents.worldbank.org/curated/en/099705012232226786/P176341132c1ef0b21adf11abad304425ef.

Committee for Payments and Market Infrastructures (CPMI) and International Organization of Securities Commissions (IOSCO), 2012. Principles for Market Infrastructures (PFMIs), Basel: Bank for International Settlements and Madrid: International Organization of Securities Commissions.

CPMI and IOSCO, 2016. Guidance on cyber resilience for financial market infrastructures. Basel: Bank for International Settlements and Madrid: International Organization of Securities Commissions.

Demirgüç-Kunt, A., Klapper, L., Singer, D., and Ansar, S. 2022. "The Global Findex Database 2021: Financial Inclusion, Digital Payments, and Resilience in the Age of COVID-19." Washington, DC: World Bank. doi:10.1596/978-1-4648-1897-4.

Department of Home Affairs (DHA). 2020. Draft official identity Management policy, public consultation version. Republic of South Africa. https://www.gov.za/sites/default/files/gcis_document/202101/44048gon1425.pdf.

Desai, V., and Clark, J. 2021. "10 principles for good ID: A 2021 refresh." World Bank Voices Blog. https://blogs.worldbank.org/en/voices/10-principles-good-id-2021-refresh

Desai, V., Marskell, J., Marin, G., and Varghese, M. 2023. "How Digital Public Infrastructure Supports Empowerment, Inclusion, and Resilience." Digital Development (blog), March 15, 2023. https://blogs.worldbank.org/digital-development/how-digital-public-infrastructure-supports-empowerment-inclusion-and-resilience.

Desai, V. T., Dolan, J. J., McGowan, K., Vora, P., Barzelay, A. M., Das, P. L., Satola, D., & Srinivasan, S. 2022. Unraveling Data's Gordian Knot: Enablers and Safeguards for Trusted Data Sharing in the New Economy. Washington, D.C.: World Bank Group. Retrieved from http://documents.worldbank.org/curated/en/863831612427670947/Unraveling-Data-s-Gordian-Knot-Enablers-and-Safeguards-for-Trusted-Data-Sharing-in-the-New-Economy.

DIGG (Sweden Agency for Digital Government). 2020. "Swedish eID: Notification form for electronic identity scheme under Article 9(5) of Regulation (EU) No 910/2014." Kingdom of Sweden. Available at https://ec.europa.eu/digital-building-blocks/sites/display/EIDCOMMUNITY/Sweden.

Dobhal, A., & Pathak, D. 2023. "India's Farmers Are on the Cusp of an Agritech Revolution: AgriStack." *World Economic Forum*, November 14, 2023. Retrieved form: https://www.weforum.org/stories/2023/11/indias-farmers-are-on-the-cusp-of-a-technological-revolution-agristack/.

Eaves, D. 2023. "Unpacking Digital Public Infrastructure and its Importance." Presentation at the Global DPI Workshop, 12 September 2023, Washington, DC. https://thedocs.worldbank.org/en/doc/98949920afb52c54cd4fc4dd15a02dbd-0050112023/original/1-1-TBS-Sept-11-DPI-presentation-edition.pdf.

Eaves, D., Mazzucato, M. and Vasconcellos, B. 2024. "Digital public infrastructure and public value: What is 'public' about DPI?" UCL Institute for Innovation and Public Purpose, Working Paper Series (IIPP WP 2024-05). https://www.ucl.ac.uk/bartlett/public-purpose/ wp2024-05.

Eichholtzer, M. 2022. "Guidance Note on Engaging Civil Society Organizations (CSOs) for Successful ID Systems" World Bank Group. https://documents1.worldbank.org/curated/en/099825009302229686/pdf/originalNames.pdf

European Union. 2014. Regulation (EU) No 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv:OJ.L_.2014.257.01.0073.01.ENG.

European Union. 2024. Regulation (EU) 2024/1183 of the European Parliament and of the Council of 11 April 2024 amending Regulation (EU) No 910/2014 as regards establishing the European Digital Identity Framework. https://eur-lex.europa.eu/eli/reg/2024/1183/oj/eng.

G20. 2023a. "Digital Economy Ministers Meeting: Outcome Document & Chair's Summary." Bengaluru, Karnataka, 19 August, 2023. https://g7g20-documents.org/database/document/2023-g20-india-sherpa-track-digital-economy-ministers-ministers-language-g20-digital-economy-ministers-meeting-outcome-document-and-chair-summary#section-3.

G20. 2023b. "G20 New Delhi Leaders' Declaration." New Delhi, India, 9-10 September 2023. https://www.mea.gov.in/Images/CPV/G20-New-Delhi-Leaders-Declaration.pdf.

Gelvanovska-Garcia, N., Mačiulė, V., and Rossotto, CM. 2024. Advancing Cloud and Data Infrastructure Markets: Strategic Directions for Low- and Middle-Income Countries. Sustainable Infrastructure Series. Washington, DC: World Bank. http://hdl.handle.net/10986/41587

GKV-Spitzenverband. Undated. "Statutory health insurance." Accessed on 22 August 2024 at https://www.gkv-spitzenverband.de/english/statutory_health_insurance/statutory_health_insurance.jsp.

GovStack Community of Practice. 2022. "GovStack Definitions: Understanding the Relationship between Digital Public Infrastructure, Building Blocks & Digital Public Goods." May 2022. https://digitalpublicgoods.net/DPI-DPG-BB-Definitions.pdf.

GovStack. 2024. "Digital Registries." Building Blocks Specifications 1.0 Publication. Retrieved from https://govstack.gitbook.io/bb-digital-registries.

Ingram, G and Vora, P. 2024. Ukraine: Digital Resilience in a Time of War. Working Paper #185. Brooking Institute. https://www.brookings.edu/wp-content/uploads/2024/01/Digital-resilience-in-a-time-of-war-Final.pdf.

Khoury, Z., Ko, Y.S., Eom, S.K., Park, K.C., Park, J.E., Cho, B., Lee, J., and Lesnichaya, Y. 2024. "Enabling Data-Driven Innovation: Learning from Korea's Data Policies and Practices for Harnessing AI." WBG Korea Office Innovation and Technology Notes. Washington, D.C.: World Bank Group. http://documents.worldbank.org/curated/en/099516201122472656/IDU15a864e96181d3149fe1993916838604fcb49.

Kumar R, Veer K. 2021. "How artificial intelligence and internet of things can aid in the distribution of COVID-19 vaccines." Diabetes Metab Syndr. 2021 May-Jun;15(3):1049-1050. doi: 10.1016/j.dsx.2021.04.021.

Lebbos, T.J., Esquivel-Korsiak, V, Clark, J. 2021. "ID Systems and SOGI Inclusive Design." Washington, DC: World Bank. https://documents.worldbank.org/en/publication/documents-reports/documentdetail/803981634587620467/id-systems-and-sogi-inclusive-design?_gl=1*1yen2x7*_gcl_au*MTczNDYzMzQ0NS4xNzIyMDAyMzc5.

Makini F.M., Mose L.O., Kamau G., Mulinge W., Salasya B., Akuku B., and Makelo M. 2020. "The Status of ICT Infrastructure, Innovative Environment and ICT4AG Services in Agriculture, Food and Nutrition in Kenya" FARA Research Report. Vol 5(11)PP 75.

Marin, G. and Palacios, R. 2022. "The Role of Digital in the COVID-19 Social Assistance Response. Washington, D.C.: World Bank Group." http://documents.worldbank.org/curated/en/099830009302217091/P1731660f8c52f062092ac00d53c648bac7.

Mbow, C., C. Rosenzweig, L.G. Barioni, T.G. Benton, M. Herrero, M. Krishnapillai, E. Liwenga, P. Pradhan, M.G. Rivera-Ferre, T. Sapkota, F.N. Tubiello, Y. Xu. 2019. "Food Security," *In: Climate Change and Land: an IPCC special report on climate change, desertification, land degradation, sustainable land management, food security, and greenhouse gas fluxes in terrestrial ecosystems* [P.R. Shukla, J. Skea, E. Calvo Buendia, V. Masson-Delmotte, H.-O. Pörtner, D.C. Roberts, P. Zhai, R. Slade, S. Connors, R. van Diemen, M. Ferrat, E. Haughey, S. Luz, S. Neogi, M. Pathak, J. Petzold, J. Portugal Pereira, P. Vyas, E. Huntley, K. Kissick, M. Belkacemi, J. Malley, (eds.)]. https://doi.org/10.1017/9781009157988.007.

Metz, A., Casher, C., and Clark, J. 2024. "ID4D Global Dataset 2021 : Volume 2 - Digital Identification Progress & Gaps." Washington, DC: World Bank. https://documents.worldbank.org/en/publication/documents-reports/documentdetail/099020824141510923/p176341192f2c50e11bc5619be95c4fb2ed?_gl=1*bwlikn*_gcl_au*MTczNDYzMzQ0NS4xNzIyMDAyMzc5.

Mifiel. 2024. "Infografía – ¿Quién tiene FIEL (Firma Electrónica Avanzada)?" Accessed on 19 August 2024 at https://blog.mifiel.com/quien-tiene-fiel/.

Mittal, A. 2022. "Catalog of Technical Standards for Digital Identification Systems." Washington, DC: World Bank Group. http://documents.worldbank.org/curated/en/707151536126464867/Catalog-of-Technical-Standards-for-Digital-Identification-Systems/.

OECD. 2024. "Developing scalable and secure digital public infrastructure", in *Government at a Glance: Latin America and the Caribbean 2024*. Paris: OECD Publishing. https://www.oecd-ilibrary.org/governance/government-at-a-glance-latin-america-and-the-caribbean-2024_4abdba16-en.

Porteous, D. 2023. "Is DPI a useful category or a shiny new distraction?" Working Paper. https://www.integralsolutionists.com/is-dpi-a-useful-category-or-a-shiny-new-distraction.

Public Digital. 2023. "Show the Thing 5: Uruguay (AGESIC) - Digital ID and digital signature." Accessed on 19 August 2024 at https://public.digital/pd-insights/blog/2023/11/show-the-thing-5-uruguay-agesic-id-uruguay-y-firma-gub-uy.

Reserve Bank of India. 2024. "Payment System Indicators." Accessed on 19 August 2024 at https://www.rbi.org.in/Scripts/PSIUserView.aspx?Id=22.

Sarkisyan, S. 2024. "Instant Payment Systems and Competition for Deposits", in Jacobs Levy Equity Management Center for Quantitative Financial Research Paper, Available at SSRN: https://ssrn.com/abstract=4176990 or http://dx.doi.org/10.2139/ssrn.4176990

Silva, M.C., Bianchi, A.G.C., Oliveira, R.A.R. and Ribeiro, S.P. 2022. "Designing a Multiple-User Wearable Edge AI system towards Human Activity Recognition," 2022 XII Brazilian Symposium on Computing Systems Engineering (SBESC), Fortaleza/CE, Brazil, 2022, pp. 1-8, doi: 10.1109/SBESC56799.2022.9964915.

Tullis, C., Constantine, N., Cooper, A. 2024. "Electronic Signatures: Enabling Trusted Digital Transformation." Digital Public Infrastructure Policy Note Series. Washington, DC: World Bank. https://hdl.handle.net/10986/42186.

Tullis, C and Black, D. 2025. "Public Key Infrastructure: Implementing High-Trust Electronic Signatures." Digital Public Infrastructure Policy Note Series. Washington, DC: World Bank. http://hdl.handle.net/10986/42663.

Tullis, C. Forthcoming. "Trusted Data Sharing: Governing Data Reuse and Value Creation." Washington, DC: World Bank.

United Nations (UN). 2023. "Extreme Poverty in Developing Countries Inextricably Linked to Global Food Insecurity Crisis, Senior Officials Tell Second Committee." Seventy-eighth Session, 16th & 17th Meetings (AM & PM), GA/EF/3590, 11 October 2023. UN Press Release. https://press.un.org/en/2023/gaef3590.doc.htm#:~:text=Agriculture%2C%20being%20the%20most%20important,families%20in%20the%20agriculture%20sector%E2%80%9D.

UN Office of the Secretary-General's Envoy on Technology (UNOSET) and UNDP. 2024. "The Universal Digital Public Infrastructure Safeguards Framework." https://dpi-safeguards-framework.org/frameworkpdf.

UNCITRAL. 2023. "UNCITRAL Model Law on the Use and Cross-border Recognition of Identity Management and Trust Services." Vienna, Austria: United Nations. https://www.un-ilibrary.org/content/books/9789210028530.

Varma, P., Matthan, R., Chaudhuri, R., and Madhukar, C.V. 2024. "The Future of Digital Public Infrastructure: A Thesis for Rapid Global Adoption." Carnegie India. https://carnegie-production-assets.s3.amazonaws.com/static/files/The_Future_of_Digital_Public_Infrastructure-_A_Thesis_for_Rapid_Global_Adoption-1.pdf.

World Bank. 2016. "World Development Report 2016: Digital Dividends." Washington, DC: World Bank. https://www.worldbank.org/en/publication/wdr2016.

World Bank. 2018. "Private Sector Economic Impacts from Identification Systems." Washington, D.C. : World Bank Group. http://documents.worldbank.org/curated/en/219201522848336907/Private-Sector-Economic-Impacts-from-Identification-Systems.

World Bank. 2019. "ID4D Practitioner's Guide." Washington, DC: World Bank. https://id4d.worldbank.org/guide.

World Bank. 2020. "Creating Disability Inclusive ID Systems." Washington, DC: World Bank. https://documents.worldbank.org/en/publication/documents-reports/documentdetail/967741605683569399/creating-disability-inclusive-id-system?_gl=1*1yen2x7*_gcl_au*MTczNDYzMzQ0NS4xNzIyMDAyMzc5

World Bank. 2021a. "World Development Report 2021: Data for Better Lives." Washington, DC: World Bank. https://www.worldbank.org/en/publication/wdr2021

World Bank. 2021b. "Considerations and Lessons for the Development and Implementation of Fast Payment Systems: Main Report." Washington DC: World Bank. https://fastpayments.worldbank.org/sites/default/files/2021-11/Fast%20Payment%20Flagship_Final_Nov%201.pdf.

World Bank. 2022a. "A Digital Stack for Transforming Service Delivery ID-Payments and Data Sharing." Washington, D.C.: World Bank Group. http://documents.worldbank.org/curated/en/099755004072288910/P1715920edb5990d60b83e037f756213782.

World Bank. 2022b. "Federated Ecosystems for Digital ID: Current Approaches and Lessons." Washington, DC: World Bank. https://documents1.worldbank.org/curated/en/099745012232218303/pdf/P17159208cf1d501a0af6f001e4852997fc.pdf.

World Bank. 2022c. "Next Generation G2P Payments : Building Blocks of a Modern G2P Architecture." Washington, DC: World Bank. https://documents.worldbank.org/en/publication/documents-reports/documentdetail/099600110202238143/p173166068e4220430a0ff03279b01c83db.

World Bank. 2022d. "Focus Note: Messaging Standards in Fast Payments" in the World Bank Fast Payments Toolkit. Finance, Competitiveness, and Innovation, Payment Systems Development Group. Washington, DC: World Bank. https://fastpayments.worldbank.org/sites/default/files/2022-03/Messaging%20Standards_Final.pdf.

World Bank. 2023. "Feature Story: Restoring Hope in Conflict-torn Northern Mozambique: Identification Documents and Livelihoods." World Bank. https://www.worldbank.org/en/news/feature/2023/08/09/restoring-hope-in-conflict-torn-afe-northern-mozambique-identification-documents-and-livelihoods.

World Bank. 2024a. *Digital Progress and Trends Report 2023*. Washington, DC: World Bank.

World Bank. 2024b. "Lebanon Digital ID Use Cases." Washington, DC: World Bank. https://documents1.worldbank.org/curated/en/099041124084041172/pdf/P1809801acb17a05c1b7f815a1a68051fa9.pdf

World Bank. 2024c. "Putting People at the Center of Digital Public Infrastructure (DPI): Annual Report 2023. Washington, DC: World Bank Group. http://documents.worldbank.org/curated/en/099647503042425828/IDU1a9d1a6be130dc148e6193181cf9d26959fb9

World Bank. 2025. "Project FASTT – Cyber risk in Fast Payment Systems". Washington, DC: World Bank Group.

World Bank and Inter-American Development Bank (IADB). 2024. "Unlocking the Potential of Digital Public Infrastructure (DPI) in Latin America and the Caribbean (LAC): A Region-Specific Perspective." A World Bank-IADB Technical Note.

WORLD BANK GROUP