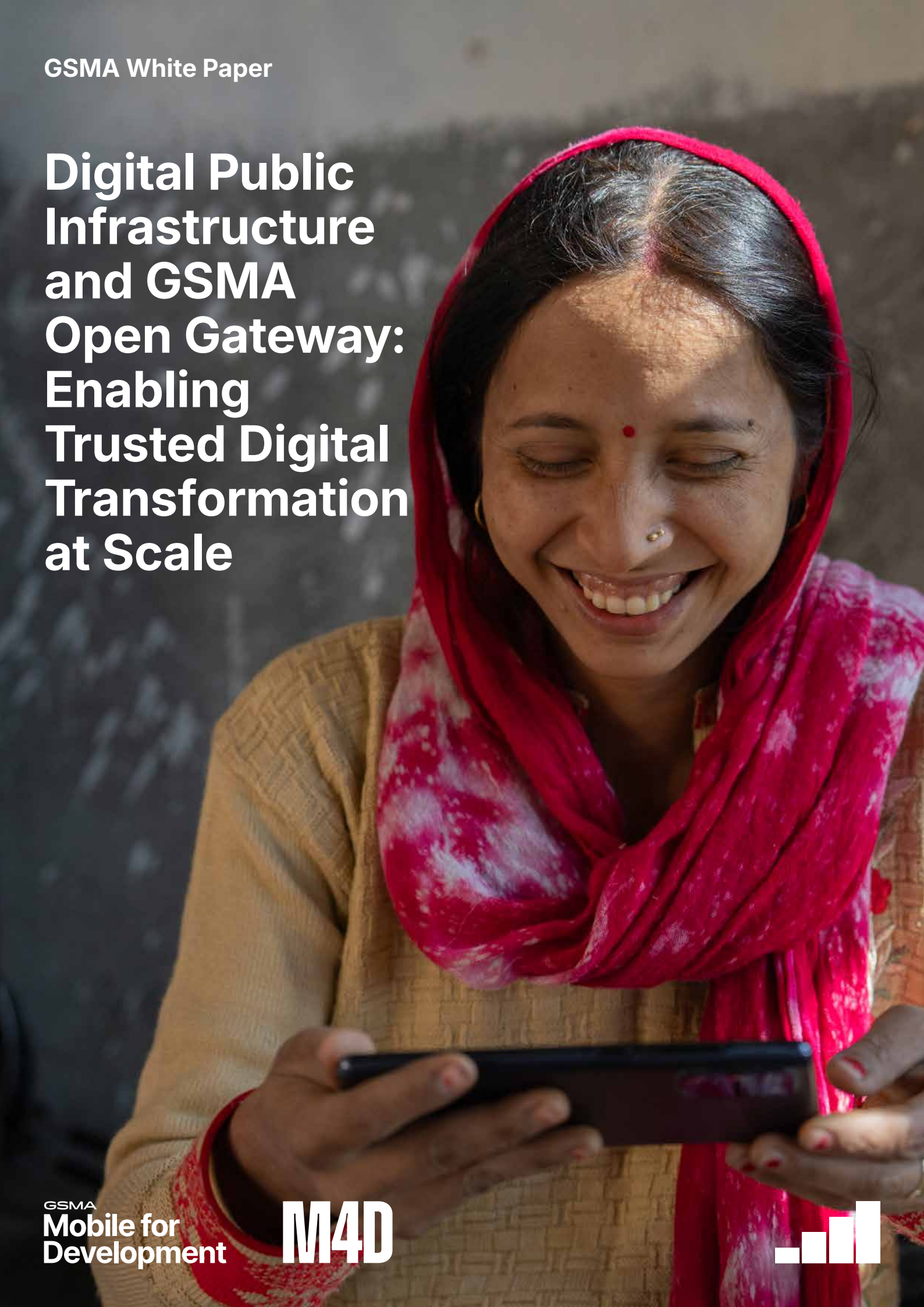
GSMA White Paper

Digital Public Infrastructure and GSMA Open Gateway: Enabling Trusted Digital Transformation at Scale



GSMA Mobile for Development

M4D

GSMA

About the GSMA
The GSMA is a global organisation unifying the mobile ecosystem to discover, develop and deliver innovation foundational to positive business environments and societal change. Our vision is to unlock the full power of connectivity so that people, industry, and society thrive. Representing mobile operators and organisations across the mobile ecosystem and adjacent industries, the GSMA delivers for its members across three broad pillars: Connectivity for Good, Industry Services and Solutions, and Outreach. This activity includes advancing policy, tackling today's biggest societal challenges, underpinning the technology and interoperability that make mobile work, and providing the world's largest platform to convene the mobile ecosystem at the MWC and M360 series of events. We invite you to find out more at gsma.com

Security classification: Public
Access to and distribution of this document is restricted to the persons permitted by the security classification. This document is confidential to the Association and is subject to copyright protection. This document is to be used only for the purposes for which it has been supplied and information contained in it must not be disclosed or in any other way made available, in whole or in part, to persons other than those permitted under the security classification without the prior written approval of the Association.

Copyright notice
Copyright © 2026 GSM Association

Disclaimer
The GSM Association ("Association") makes no representation, warranty or undertaking (express or implied) with respect to and does not accept any responsibility for, and hereby disclaims liability for the accuracy or completeness or timeliness of the information contained in this document. The information contained in this document may be subject to change without prior notice.

Note: This white paper explores how GSMA Open Gateway capabilities can complement digital public infrastructure (DPI) initiatives. It is intended to inform discussion and does not constitute a GSMA policy position or endorsement of any specific DPI initiative, architecture or implementation approach.

GSMA Inclusive Digital Finance

The GSMA's Inclusive Digital Finance programme works to drive an inclusive digital finance ecosystem by mobilising providers, policymakers and partners to deliver market innovation and reform, closing the gap between financial access and genuine financial health for underserved populations.

For more information, please contact us:
www.gsma.com/inclusive-digital-finance

Antitrust notice
The information contain herein is in full compliance with the GSM Association's antitrust compliance policy.

Unlock the benefits of GSMA membership
As a member of the GSMA, you join a vibrant community of industry leaders and visionaries – helping to shape the future of mobile technology and its transformative impact on societies worldwide.

Our unique position at the heart of the mobile industry means you get exclusive access to our technical experts, data and analysis, as well as unrivalled opportunities for networking, innovation support and skills acceleration.

For more information, please visit: gsma.com/get-involved

Author:
Soheib Nunhuck, GSMA

Contributing GSMA teams:
Mobile for Development, External Affairs, Foundry, Open Gateway, Policy & Regulatory and Marketing

Published: September 2026

CONTENTS

Executive summary 4

1. Introduction 5

2. Mobile networks: integral to DPI 7

3. GSMA Open Gateway: mobilising trusted network capabilities for DPI 8

4. How GSMA Open Gateway can strengthen core DPI systems 10

4.1 Reinforcing trust in digital identity 10

4.2 Strengthening trust across the payment life cycle 11

4.3 Strengthening trust in digital interactions 11

4.4 From examples to future opportunities 12

5. From infrastructure to trusted digital ecosystems 13

EXECUTIVE SUMMARY

Digital public infrastructure (DPI) has become an important approach to digital transformation, with countries around the world pursuing implementation models that reflect their development priorities, governance arrangements and digital sovereignty objectives. From interoperable digital identity to payments and trusted data exchange systems, DPI provides a common foundation for secure, scalable and accessible digital services. Like mobile networks and the internet before it, DPI has the greatest impact when users can access it securely, transparently and responsibly, and when it enables innovation, strengthens interoperability, improves services and supports broad participation in the digital ecosystem.

This white paper examines the role of the GSMA Open Gateway in DPI ecosystems and highlights the strategic opportunity for the mobile industry to support the next phase of DPI development. Rather than taking a position on national DPI models and initiatives, it explores how existing mobile network capabilities can be securely reused through a global framework of common network application programming interfaces (APIs) to complement national digital identity, digital payments and trusted data exchange initiatives. Drawing on practical deployments, this paper illustrates how these capabilities can strengthen trust, improve interoperability and help countries build more resilient and inclusive digital ecosystems.



1. INTRODUCTION

Digital public infrastructure (DPI) represents a new approach to digital transformation at scale, centred on three foundational and interoperable systems: digital identity, digital payments and data exchange. Built as reusable and modular infrastructure, these systems enable governments, businesses and citizens to interact more securely and efficiently. Unlike traditional digital transformation initiatives, DPI provides a common foundation that can be reused and expanded across public and private services, accelerating innovation while reducing duplication, technology lock-in and long-term costs.[1] Today, most countries have implemented or are piloting at least one core DPI system, making DPI a policy priority.[2]

The individual components of DPI are not new. Digital identity, payments and data exchange systems have evolved independently over many years through public- and private-sector investment and innovation. What is new is that DPI brings these systems together as reusable foundations for digital transformation. It represents a shift from stand-alone digital initiatives to shared infrastructure that can support trusted ecosystems, innovation and the scalable delivery of public and private services. Unlike previous generations of digital infrastructure, their long-term success depends not only on the technologies deployed, but also on the interoperability that enables others to build upon them. Countries will pursue implementation models based on their development priorities, governance arrangements, digital maturity and sovereignty objectives. While these approaches will differ, they share a common ambition: leveraging trusted digital infrastructure to improve service delivery, strengthen digital economies and support inclusive growth.

Digital identity, payments and trusted data exchange provide the building blocks of digital economies, but their greatest value comes from governments, businesses and citizens adopting and reusing them for everyday services. This requires resilient communications infrastructure, reliable connectivity, affordable devices, digital skills and interoperability across sectors. History shows that digital infrastructure has had the greatest impact when it enables entire ecosystems to build, adapt and innovate. Successful DPI should therefore be measured not only by the infrastructure built and governed, but by the extent to which it enables trusted interactions, widespread adoption and tangible social and economic outcomes.

Recent discussions have rightly explored what makes DPI "public".[3] Equally important is understanding what makes DPI trusted. Governments play a central role in defining national priorities, establishing governance arrangements and stewarding the development of DPI systems in the public interest. However, trust cannot be built by government alone. It also depends on a wider ecosystem of actors whose capabilities, standards and operational experience enable trusted digital interactions at scale. Mobile network operators (MNOs) are particularly well placed to contribute. Through decades of investment and industry-wide collaboration, they already provide authentication, identity verification, fraud prevention, secure communications and digital financial services (DFS) in many markets. Within DPI ecosystems, MNOs can be understood not only as providers of connectivity, but as participants whose capabilities can enhance the value of foundational DPI systems.

1. Clark, J. et al. (2025). Digital Public Infrastructure and Development: A World Bank Group Approach – Digital Transformation White Paper: Volume 1. World Bank Group.
2. Eaves, D. and Rao, K. (2025). Digital Public Infrastructure: a framework for conceptualisation and measurement. UCL Institute for Innovation and Public Purpose, Working Paper Series (IIPP WP 2025-01).
3. Mazzucato, M., Eaves, D. 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).

GSMA Open Gateway complements DPI ambitions by providing a common protocol for trusted digital interactions. Through globally interoperable network application programming interfaces (APIs), it enables governments, enterprises and developers to securely access mobile network capabilities across operators and markets. While considerable attention has been given to how countries should design, implement and govern DPI systems, less attention has been paid to how trusted capabilities that already exist within digital ecosystems can reinforce national DPI strategies. This paper examines that opportunity.

The central argument of this paper is that GSMA Open Gateway is not another core DPI system, nor does it advocate for a particular national approach to DPI. Rather, it provides a practical mechanism for extending trusted mobile network capabilities into DPI ecosystems through common and interoperable protocols while preserving national ownership, flexibility and technology neutrality. This paper does not advocate for a particular DPI model or for DPI as the preferred approach to national digital transformation; rather, it examines how existing mobile network capabilities may be relevant in countries that choose to develop DPI or DPI-like systems.

This white paper examines how capabilities originally developed for commercial digital services can reinforce core DPI systems and outlines the potential role of the mobile industry as a strategic participant in DPI ecosystems. It begins by establishing how the mobile industry is integral to the evolution of DPI before exploring how GSMA Open Gateway enables these capabilities to be securely reused across operators, sectors and markets. It then demonstrates this contribution through examples before reflecting on the broader transition from foundational infrastructure to trusted digital ecosystems.



2. MOBILE NETWORKS: INTEGRAL TO DPI

The mobile industry offers a useful reference point for DPI because it demonstrates how infrastructure evolves into ecosystems through standards, governance, long-term investment and broad ecosystem participation. Over decades, mobile networks have evolved from communications infrastructure into trusted digital ecosystems. This transformation was driven not only by connectivity, but by the trusted capabilities, interoperable standards and innovation that developed around it. In many respects, the mobile industry has already navigated the transition from infrastructure to ecosystem that DPI is only beginning. Its experience therefore offers valuable lessons for designing trusted, inclusive and sustainable digital ecosystems.

This evolution has been underpinned by trusted capabilities that now form an essential part of digital economies. Beyond connectivity, MNOs provide secure authentication, identity and device verification, fraud prevention, trusted communications and DFS on a national scale. Through sustained investment, they have expanded digital access, helped narrow coverage and usage gaps and built long-standing public-private partnerships alongside customer relationships that depend on security, reliability and consumer trust. Their relevance to DPI lies not simply in the scale of mobile networks, but in the combination of reach, operational maturity and trusted customer relationships they have developed over time. As such, MNOs can bring capabilities, scale and operational experience to DPI ecosystems in ways that few other actors can match, supporting design, implementation and long-term sustainability.

The mobile industry has repeatedly demonstrated that competing actors can collaborate on open standards while continuing to innovate and compete.[4] This balance between interoperability and competition provides a useful model for DPI, as shared digital infrastructure must enable both public value and sustainable private-sector participation.

For DPI, the key opportunity is to reuse existing capabilities rather than duplicating them. MNOs have developed practical expertise in operating critical infrastructure, managing trusted digital services and sustaining commercially viable ecosystems over time. Importantly, these capabilities have evolved in response to real consumer, business and public sector needs, with the mobile industry translating user demand into trusted digital services at scale. This experience is directly relevant to DPI challenges such as adoption, resilience, interoperability, fraud prevention and financial sustainability. Because these capabilities already operate at scale across digital economies, they can complement national DPI systems without displacing public governance.

Mobile money illustrates how trusted digital ecosystems emerge. Originally developed to address financial inclusion challenges, it has become a critical enabler for people and businesses historically excluded from formal financial systems.[5] By giving users a trusted and easy way to store, send and receive money, mobile money has helped bring informal economic activity into more formal digital channels while supporting commerce, social protection and broader economic participation. It also provides an important lesson for DPI: that foundational technology only has a positive impact when it is embedded in a wider ecosystem that supports adoption, trust, interoperability and sustainable growth. The same conditions will determine whether DPI evolves beyond foundational systems into widely adopted digital ecosystems.

Just as GSM established a globally interoperable foundation for mobile communications, and HTTP enabled seamless interactions across the internet, DPI ecosystems will increasingly require common protocols for establishing trusted digital interactions across sectors and markets. GSMA Open Gateway represents the next phase of industry mobilisation, providing common, interoperable network APIs that are accessible, reusable and scalable across user-centric digital services.

4. GSMA. (2024). Mobile Policy Handbook 2024: An insider's guide to the issues.
5. GSMA. (2026). The State of the Industry Report on Mobile Money 2026.

3. GSMA OPEN GATEWAY: MOBILISING TRUSTED NETWORK CAPABILITIES FOR DPI

The GSMA is a global organisation representing the mobile ecosystem, bringing together MNOs, technology providers and industry stakeholders to advance interoperability and the mobile industry's collective interests. One of its flagship industry initiatives is GSMA Open Gateway initiative, a global framework of common, interoperable network APIs that simplifies access to mobile operator networks and helps expose core capabilities of the open network to developers and cloud providers.

Through GSMA Open Gateway, MNOs identify network capabilities that enterprises and developers want access to. The GSMA Operator Platform Group cooperates with CAMARA, an open-source project within Linux Foundation that defines, develops and tests the APIs, aligning API requirements and publishing definitions. API harmonisation is achieved through an agile, open-source development process that produces consistent API definitions, reference implementations and developer-friendly documentation. A key focus has been the development of APIs to support authentication, identity verification, device verification, fraud prevention and location-based assurance in a secure, interoperable way for MNOs and technology partners, subject to applicable legal, regulatory and consumer protection requirements. Open Gateway reflects the same principles that underpin DPI: openness, interoperability, modularity and reusability.

For countries pursuing DPI, GSMA Open Gateway has become increasingly relevant. While Open Gateway was originally designed to simplify access to trusted mobile network capabilities, as DPI has matured, these capabilities can also reinforce national digital ecosystems. Rather than introducing another DPI layer in the traditional sense, it makes capabilities that already operate at scale easier to reuse across digital identity, payments, trusted data exchange and other emerging public and private digital services. This can simplify implementation, avoid duplication and help DPI stakeholders build on trusted infrastructure already embedded within national digital economies. Its value therefore lies in providing a consistent framework through which these capabilities can be securely accessed and reused across different systems, sectors and markets. For MNOs, it also provides a practical mechanism to support national digital transformation initiatives, enhancing the value of trusted network capabilities and ultimately strengthening the business case for continued investment and innovation.

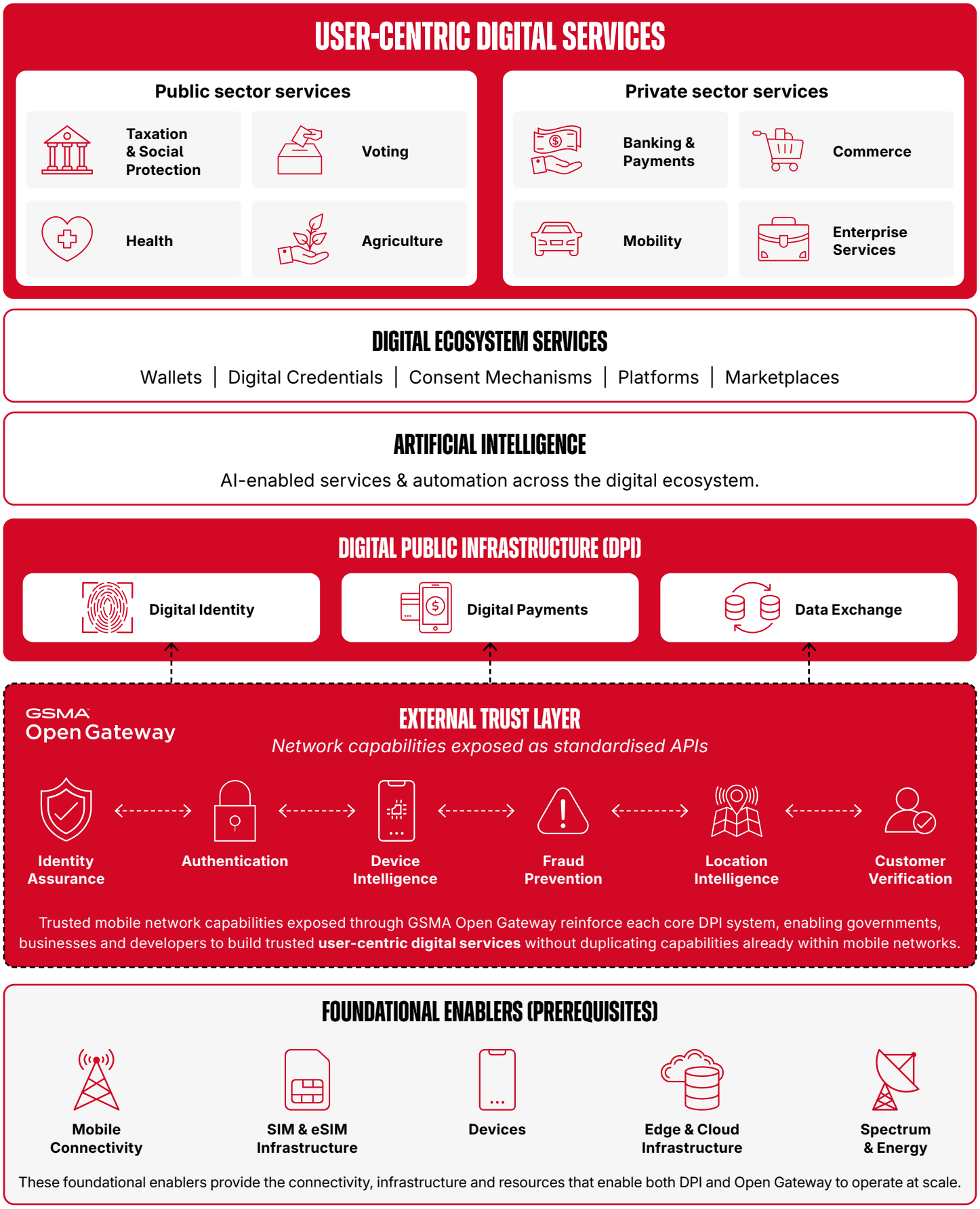
GSMA Open Gateway also aligns with broader global discussions on trust in DPI. The United Nations DPI Safeguards Initiative emphasises that DPI should protect rights, reduce risks and build trust across governance, design, deployment and use.[6] While Open Gateway is not a safeguards framework, it can support these objectives by making capabilities such as identity assurance, fraud prevention, secure digital interactions and service reliability more accessible through standardised APIs. Their contribution to DPI will nevertheless depend on appropriate governance, regulation and rights-based oversight. These capabilities can also contribute to the cybersecurity of services built around DPI by providing network-derived signals that can detect suspicious activity and reduce risks such as account takeover and other identity fraud. They do not replace critical cybersecurity measures within DPI systems themselves but can provide an additional layer of assurance around the digital interactions that depend on them.

As illustrated in Figure 1, GSMA Open Gateway acts as a common, interoperable framework through which existing mobile network capabilities can complement each of the core DPI systems. The illustration is conceptual and should not be interpreted as prescribing a reference architecture for national DPI implementations. The APIs shown demonstrate how the same trusted capability can support more than one DPI component, reflecting the modular and reusable architecture that underpins both DPI and GSMA Open Gateway.

6. United Nations Office of the Secretary-General's Envoy on Technology (OSET) and United Nations Development Programme (UNDP). (2024). The Universal DPI Safeguards Framework: A Guide to Building Safe and Inclusive Digital Public Infrastructure.

Figure 1

Establishing GSMA Open Gateway within the wider DPI context



Note: The trusted mobile network capabilities illustrated here are representative examples of how GSMA Open Gateway can reinforce DPI. They do not represent the full Open Gateway API portfolio, nor the full range of existing and emerging DPI use cases that these capabilities may support.

4. HOW GSMA OPEN GATEWAY CAN STRENGTHEN CORE DPI SYSTEMS

The following examples illustrate how mobile network capabilities can strengthen different components of DPI.[7] Although many capabilities can support more than one DPI function, each example is grouped by its primary contribution. Together, they help identify where similar opportunities may emerge as Open Gateway adoption expands across more markets. In considering these examples, the reuse of network capabilities should be understood alongside the importance of privacy, transparency, user control and security.

4.1 Reinforcing trust in digital identity

Digital identity is a core DPI component as it enables people to prove who they are and access services securely. However, trust must be maintained across the full identity life cycle, from onboarding and authentication to account recovery and ongoing verification. GSMA Open Gateway can complement national digital identity systems by making mobile network capabilities available through common interfaces that strengthen identity assurance, improve user experience and reduce fraud. Rather than replacing these systems, it enables governments and service providers to draw on trusted capabilities that already exist within mobile networks.

GSMA Open Gateway	Example deployment	DPI use case	Contribution to digital identity
Number verification[8]	Dialog Axiata (Sri Lanka)	Citizen authentication for digital services (e.g. LankaPay)	Enables silent authentication by confirming possession of a registered mobile number, strengthening identity assurance while improving user experience.
KYC match[9]	Orange, Bouygues Telecom, Free, SFR (France)	Digital identity enrolment (eKYC)	Validates customer information against trusted MNO records, strengthening identity verification during onboarding.
Age verification[10]	BT/EE, Virgin Media, O2, Vodafone	Age assurance for digital services	Confirms whether a user meets a required age threshold using MNO-verified data, supporting privacy-preserving access to age-restricted digital services.
Integrated Identity APIs (Number Verification, KYC Match, SIM Swap & Device Roaming Status)[11]	MID Plus – Chunghwa Telecom, Taiwan Mobile and Far EasTone (Taiwan)	Mobile identity and trusted digital services	Combines multiple trusted mobile network capabilities to strengthen identity verification, user authentication and fraud prevention, supporting a trusted mobile identity ecosystem for digital services.

7. GSMA. (2026). GSMA Open Gateway Roadmap.
8. GSMA. (2025). LankaPay protects payment accounts from takeovers. GSMA Open Gateway Case Study.
9. GSMA. (2025). French mobile industry accelerates deployment of network APIs through GSMA Open Gateway Initiative. GSMA Open Gateway Case Study.
10. GSMA. (23 September 2025). "UK Mobile Operators Launch Age Verification and Anti-Fraud APIs Through GSMA Open Gateway Initiative". Press release.
11. GSMA. (2 July 2026). "Telecom and Financial Sectors Join Forces Against Scams as Taiwan Launches GSMA Open Gateway APIs".

4.2 Strengthening trust across the payment life cycle

Digital payment systems enable people, businesses and governments to exchange value securely and efficiently. As payments become more real time, digital and interconnected, fraud risks also become more dynamic. Trust therefore needs to be maintained across the full payment life cycle, from onboarding and authentication to transaction approval and account recovery. GSMA Open Gateway can complement digital payment systems by making mobile network capabilities available through common interfaces that strengthen transaction integrity, reduce fraud and improve confidence without changing the underlying payment infrastructure.

GSMA Open Gateway	Example deployment	DPI use case	Contribution to digital payments
SIM swap[12]	Itaú (Brazil)	Payment fraud prevention	Detects recent SIM replacement before authorising high-risk transactions, reducing account takeover and payment fraud.
Number verification[13]	Banco Daycoval (Brazil)	Customer onboarding	Simplifies secure onboarding and customer verification for DFS.
Device swap[14]	China Mobile (China)	Payment security and fraud prevention	Detects changes to a customer's trusted device following theft or replacement, providing additional trust signal to support payment authorisation, account recovery and fraud mitigation.

4.3 Strengthening trust in digital interactions

Trusted data exchange enables information to move securely between people, businesses and governments, underpinning digital services across sectors such as healthcare, education, mobility and public administration. As these services become increasingly interconnected, trust depends not only on protecting data, but also on establishing confidence in the users, devices, networks and conditions involved in each interaction. GSMA Open Gateway can complement trusted data exchange by making mobile network capabilities available through common APIs that provide additional trust signals, enabling more secure, reliable and context-aware digital services.

GSMA Open Gateway	Example deployment	DPI use case	Contribution to data exchange
Quality on demand[15]	Alibaba Cloud (China)	Reliable digital transactions and digital public services	Dynamically enhanced network quality during mobile payment transactions, helping ensure digital interactions are completed reliably and strengthening user trust in digital service delivery.
Quality on demand[16]	AECC	Connected and intelligent transport services	Enables guaranteed network performance for connected vehicle services, improving service reliability and strengthening consumer confidence in safety-critical digital interactions.
Location verification[17]	Banco Daycoval (Brazil)	Fraud prevention for DFS	Verifies that a customer's device is located where expected before authorising sensitive digital interactions, reducing fraud risk and providing an additional trust signal for secure digital services.

12. GSMA. (2025). Brazilian Operators: Advancing Digital Trust through Mobile Network APIs. GSMA Open Gateway Case Study.
13. Ibid.
14. GSMA. (2025). China Mobile Simplifies Customer Registration with Phone Number Verification. GSMA Open Gateway Case Study
15. GSMA. (2025). Alibaba Cloud Increases the Reliability of Mobile Payments. GSMA Open Gateway Case Study.
16. GSMA. (2026). AECC Enhances Connected Vehicle Services with Quality on Demand. GSMA Open Gateway Case Study.
17. GSMA. (2025). Banco Daycoval Taps Location Data to Reduce Fraud. GSMA Open Gateway Case Study.

4.4 From examples to future opportunities

The examples in this section demonstrate how trusted mobile network capabilities standardised and deployed through GSMA Open Gateway can address important trust issues with DPI. They also reflect growing demand from digital services for capabilities such as identity assurance, fraud prevention, secure interactions and service reliability. Rather than illustrating isolated deployments, they reveal a broader pattern: capabilities originally developed to support commercial digital services are increasingly aligned with the functional requirements of mature DPI ecosystems. This should not be interpreted as evidence that national DPI programmes are already leveraging GSMA Open Gateway. Rather, it signals growing mobile industry readiness and highlights where existing capabilities may support future DPI implementation.

Looking ahead, additional capabilities such as consent management illustrate how this opportunity could evolve. As DPI ecosystems mature, trusted mechanisms for capturing, managing and revoking consent are increasingly recognised as essential to secure and user-centric data exchange. Meaningful consent extends beyond obtaining permission; it requires transparent, informed and revocable mechanisms that enable individuals to understand and control how their data is used.[18] While consent management currently underpins the technical architecture supporting Open Gateway APIs – rather than existing as a stand-alone commercial capability – it illustrates how standardised network capabilities could increasingly support trusted data exchange across sectors.[19] This could help verify that an authorised user or account holder has granted permission under defined conditions and for a specific purpose, strengthening trust in digital interactions. Beyond consumer-facing services, similar authorisation mechanisms could also support enterprise and Internet of Things (IoT) use cases, where trusted verification of devices, services or system interactions is essential for secure automated exchanges.

As DPI agendas mature, the focus will shift from establishing foundational systems to enabling trusted interactions across a range of public and private digital services. In this context, GSMA Open Gateway offers a practical way to securely reuse existing mobile network capabilities, allowing governments, enterprises and developers to build on trusted capabilities that already operate at scale rather than recreate them.

This opportunity extends beyond markets where Open Gateway capabilities are already commercially available. In a growing number of countries, MNOs are aligning around Open Gateway through GSMA Market Champion initiatives, demonstrating a collective industry commitment to exposing trusted mobile network capabilities through open and standardised protocols. These initiatives indicate that MNOs are preparing capabilities in response to market demand and potential local needs. Markets where MNOs are doing this collectively for tangible business outcomes may offer promising opportunities for future engagement as national DPI strategies mature.

The practical implication is simple: governments developing DPI should engage MNOs early. Existing mobile network capabilities may already support some of the trust, security and interoperability needs of DPI. GSMA Open Gateway provides one way to make those capabilities easier to access and reuse, without prescribing a specific DPI model or technology path. Doing so offers an opportunity to strengthen trust, improve interoperability and mobilise existing capabilities from the mobile ecosystem while preserving flexibility, technology neutrality and long-term sustainability.

18. Digital Impact Alliance. (10 December 2024). "Good digital public infrastructure relies on effective consent mechanisms. Here's how they work."
19. GSMA. (2026). OPG.10 – Open Gateway Technical Realisation Guidelines.

5. FROM INFRASTRUCTURE TO TRUSTED DIGITAL ECOSYSTEMS

The long-term success of DPI will not only depend on the infrastructure countries build, but on the trusted digital ecosystems those systems enable. As public and private services continue to expand, and as societies seek to improve service delivery, accelerate innovation and harness emerging technologies such as AI, trust becomes the defining characteristic of mature digital ecosystems.

History shows that technologies have the greatest societal impact when they evolve into shared infrastructure. Mobile networks and the internet transformed economies at their core because these technologies became open, interoperable foundations on which others could build. DPI is approaching a similar moment, and its long-term value will depend on whether infrastructure can support trusted interactions and sustained innovation by the wider digital ecosystem. GSMA Open Gateway shows how common network APIs can expose trusted mobile capabilities for reuse across markets, enhancing the value of DPI without duplicating existing infrastructure.

Ultimately, interoperability transforms infrastructure into ecosystems. By enabling trusted capabilities to be reused across sectors, common network APIs allow governments, businesses and developers to build on shared foundations while preserving flexibility and innovation. For countries pursuing DPI, this supports a more durable form of digital sovereignty: not dependence on a single technology path, but the ability to build trusted, resilient and adaptable ecosystems on their own terms. The next phase of DPI will be defined by trust – how it is built, shared and scaled.



GSMA Head Office
1 Angel Lane
London EC4R 3AB
United Kingdom

gsma.com

GSMA
Mobile for Development

M4D