

Public Disclosure Authorized



Public Disclosure Authorized

JORDAN

DIGITAL PUBLIC INFRASTRUCTURE DIAGNOSTIC

Public Disclosure Authorized

Public Disclosure Authorized



December 2024
Digital Vice Presidency Unit



© 2024 The World Bank
1818 H Street NW, Washington DC 20433
Telephone: +1-202-473-1000; Internet: www.worldbank.org

Some rights reserved.

This work is a product of The World Bank. The findings, interpretations, and conclusions expressed in this work do not necessarily reflect the views of the Executive Directors of The World Bank or the governments they represent.

The World Bank does not guarantee the accuracy, completeness, or currency of the data included in this work and does not assume responsibility for any errors, omissions, or discrepancies in the information, or liability with respect to the use of or failure to use the information, methods, processes, or conclusions set forth. The boundaries, colors, denominations, links/footnotes and other information shown in this work do not imply any judgment on the part of The World Bank concerning the legal status of any territory or the endorsement or acceptance of such boundaries. The citation of works authored by others does not mean the World Bank endorses the views expressed by those authors or the content of their works.

Nothing herein shall constitute or be construed or considered to be a limitation upon or waiver of the privileges and immunities of The World Bank, all of which are specifically reserved.

Rights and Permissions

The material in this work is subject to copyright. Because The World Bank encourages dissemination of its knowledge, this work may be reproduced, in whole or in part, for noncommercial purposes as long as full attribution to this work is given. Cover photo: © Shutterstock, Inc. Used with the permission of Shutterstock, Inc. Further permission required for reuse. Cover Design: [add name here]

Attribution - Please cite the work as follows: "Tullis, Christopher. 2024. Jordan Digital Public Infrastructure Diagnostic. © Washington, DC: World Bank."

Any queries on rights and licenses, including subsidiary rights, should be addressed to World Bank Publications, The World Bank, 1818 H Street NW, Washington, DC 20433, USA; fax: +1-202-522-2625; e-mail: pubrights@worldbank.org.

Cover photo: © Ministry of Digital Economy and Entrepreneurship, Hashemite Kingdom of Jordan. Used with the permission of Ministry of Digital Economy and Entrepreneurship, Hashemite Kingdom of Jordan. Further permission required for reuse.

Cover design: Duina

TABLE OF CONTENTS

	About ID4D	4
	Acknowledgments	5
	1. Introduction	6
	2. Foundations and enablers	10
	2.1 Legal identity	10
	2.2 Data centers and cloud computing	11
	2.3 Legal and regulatory framework	12
	3. Digital ID & Trust services	14
	3.1 Digital identity	14
	3.2 Electronic signature	17
	3.3 Public key infrastructure	18
	3.4 Consent management	18
	4. Data sharing	20
	4.1 Direct data sharing	20
	4.2 Decentralized data sharing	20
	4.3 Data aggregation	23
	5. Use cases	24
	5.1 Sanad e-services portal	24
	6. Conclusions	26

ABOUT ID4D

The World Bank's Identification for Development (ID4D) Initiative harnesses global and cross-sectoral knowledge, World Bank financing instruments, and partnerships to help countries realize the transformational potential of identification (ID) systems, including civil registration (CR). The aim is to enable all people to exercise their rights and access better services and economic opportunities in line with the Sustainable Development Goals.

ID4D operates across the World Bank with global practices and units working on digital development, social protection, health, financial inclusion, governance, gender, and data protection, among others. To ensure alignment with international good practices for maximizing development benefits and minimizing risks, ID4D is guided by the 10 Principles on Identification for Sustainable Development, which has been jointly developed and endorsed by the World Bank and over 30 global and regional organizations (see <http://idprinciples.org>).

ID4D makes this happen through its three work pillars:

1. Thought leadership, research, and analytics to generate evidence and fill knowledge gaps.
2. Global public goods and convening to develop and amplify good practices, foster collaboration across regional and global stakeholders, and support knowledge exchange.
3. Country and regional action through financial and technical assistance to realize inclusive and trusted ID and civil registration systems.

The work of ID4D is made possible through support from the Bill & Melinda Gates Foundation, the UK Government, The French Government, The Norwegian Agency for Development Cooperation (NORAD), and the Omidyar Network. To find out more about ID4D and access our other publications, visit <https://id4d.worldbank.org/>



ACKNOWLEDGMENTS

This report was authored by Christopher Tullis, Senior Digital Development Specialist in the World Bank's Digital Vice Presidency Unit. It is the result of collaboration between the World Bank's Identification for Development (ID4D) Initiative and Jordan's Ministry of Digital Economy and Entrepreneurship (MoDEE). Excellent feedback and inputs were provided throughout the development of this report. Thanks go to H.E. Ahmad Hanandeh, Minister of Digital Economy and Entrepreneurship, as well as the following individuals (listed in alphabetical order) for their various contributions: Ayman Anabtawi, Ahmad Elayyan, Ahlam Jadallah, Yousef Khamees, and Ramy Rawashdih (MoDEE); Ibrahim Mbaidin (Ministry of Planning and International Cooperation); and Abdallah Jabbour, Nay Constantine, Ambrose Wong, David Porteus, Nadine Chehade, and Matthew Zoller (World Bank). Thoughtful peer reviews by Julia Clark, Stephen Davenport, and Samer Qubain also helped improve the quality of this report.



1 INTRODUCTION

In recent years, Jordan has increasingly strengthened its commitment to enhancing public service delivery through digital public infrastructure (DPI). DPI refers to foundational and reusable digital platforms and building blocks—such as digital ID, digital payments, and data sharing—that underpin the development and delivery of trusted, digitally-enabled services across the public and private sectors, including social protection, health, public finance, and banking.¹ Jordan’s National Digital Transformation Strategy and Implementation Plan for 2021-2025² reflects the country’s strategic commitment, with the Government actively establishing DPI building blocks, such as digital identity and data sharing platforms to accelerate the digitalization of public services using a secure and scalable architecture.

Despite these increased efforts, the adoption of digitalized public services remains limited. Only about 1.4 million Jordanians are registered on Sanad, the integrated e-services platform that is central to the country’s digital public service delivery.³ Service uptake is hindered by limited practical use cases, optionality of digital service usage, and inability to complete digital transactions end-to-end for many public services.

Recognizing these hurdles, the World Bank’s Digital team conducted several missions in 2023 to assess the technical gaps in establishing a trusted, people-centric DPI ecosystem in Jordan, ensuring that all residents, including non-Jordanians and refugees, can fully benefit from digital public services. In addition to looking at core DPI components, such

as digital ID and data sharing; the missions also examined foundational enablers crucial to DPI implementation. Digital payments were excluded from the scope as they will be specifically addressed by forthcoming complementary work on the subject. The team engaged in comprehensive discussions with the Ministry of Digital Economy and Entrepreneurship (MoDEE) to examine the challenges and opportunities associated with the DPI ecosystem and the digital public services it enables. This diagnostic report summarizes those discussions and contributes to the analytical groundwork for the Jordan People-Centric Digital Government Program for Results (P180291). Approved by the World Bank’s Board of Directors in March 2024 and effective as of June 2024, the program aims to enhance people-centric service delivery, government effectiveness, and transparency and accountability through digitalization.

This diagnostic provides a comprehensive review of the digital public service delivery enabled by Jordan’s DPI ecosystem and presents recommendations on features that bolster trust, interoperability, security, and people centricity.⁴ To better understand the ecosystem’s components, a simplified, high-level overview of how these building blocks interconnect is presented in Figure 1:

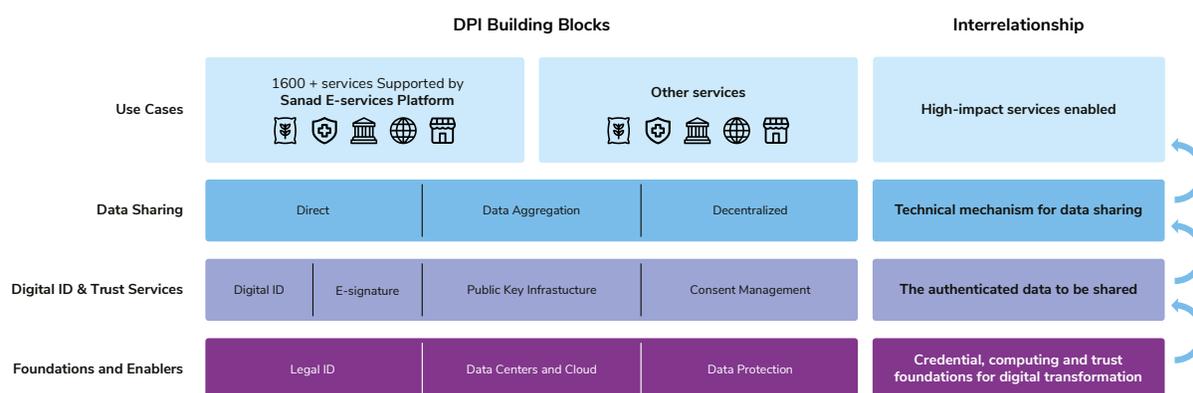
1 DPI is not a replacement for sector-specific digital data or infrastructure—e.g., digital registries for social protection, credit, agriculture, health-sector interoperability and data exchange standards; digital tax or HR MIS, etc.—rather, DPI helps enable and scale sector-owned digital services that rely on sector-owned assets quicker, cheaper, more reliably, and more sustainably.

2 The Hashemite Kingdom of Jordan, Ministry of Digital Economy & Entrepreneurship, The National Digital Transformation Strategy & Implementation Plan (2021-2025). Available at https://www.modee.gov.jo/ebv4.0/root_storage/en/eb_list_page/dts-2021-eng.pdf

3 This represents approximately 37 percent of individuals aged 16 or above who also have a smart national ID, biometric iris registration, or bank account, and approximately 19 percent of individuals over 16 who are eligible to activate the Sanad Digital ID feature (but may or may not have a smart national ID, biometric iris registration, or bank account)

4 Interoperability is the ability of one entity to communicate with another. For more information, see Guideline for Using Cryptographic Standards in the Federal Government: Cryptographic Mechanisms. National Institute of Standards and Technology. U.S. Department of Commerce. <https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-175Br1.pdf>

Figure 1: Layered model of digital trust



The findings from this comprehensive and systematic diagnostic will help the Jordanian Government advance toward a trusted, people-centric DPI ecosystem, spurring user adoption and accelerating the country’s digital transformation. To this end, Table 1 provides a snapshot of this diagnostic’s main suggestions.

Table 1. Recommendations for Jordan’s DPI Ecosystem - A Snapshot

Summary of Recommendations	
1. FOUNDATIONS AND ENABLERS	
Legal Identity	<ul style="list-style-type: none"> Strengthen the credentials used for onboarding of non-Jordanians (residents and refugees), military personnel, and potentially tourists. Render Jordan’s national ID system (i.e., MoI database) interoperable with UNHCR’s systems to simplify the issuance process of service cards for refugees. Deploy mobile registration centers to camps and UNHCR registration centers to facilitate large-scale onboarding of refugees onto Sanad.
Data Centers and Cloud	<ul style="list-style-type: none"> Conduct stakeholder consultations with ministries, departments, and agencies (MDAs) to better identify barriers to cloud adoption. Refine the Cloud Policy⁵ continuously to increase the flexibility of using both national and international public cloud providers for less sensitive data.
Data Protection	<p>Incorporate the following recommendations in a future revision to the Personal Data Protection Law⁶ or the adoption of secondary legislation, such as implementing decrees:</p> <ul style="list-style-type: none"> Introduce good-practice concepts such as data minimization and privacy impact assessments. Reduce the number and scope of exemptions for public-sector entities to share and process data without a clear legal basis. Improve the independence of the data protection authority and improve the alignment of its governance model with international good practice.

5 The Hashemite Kingdom of Jordan, Ministry of Digital Economy & Entrepreneurship (2020), Cloud (Platforms & Services) Policy. Available at https://www.modee.gov.jo/ebv4.0/root_storage/en/eb_list_page/cloudpolicy-2020-english.pdf.

6 Law No. 24 of 2023 regarding personal data protection, published in the Official Gazette on 17 September 2023.

2. DIGITAL ID AND TRUST SERVICES

Digital Identity	<ul style="list-style-type: none">• Carry out consultations to identify and address barriers to adoption of the Sanad digital ID, including single sign-on (SSO)⁷ features, and establish methods of integration into their service delivery workflows and business processes.• Accelerate ongoing efforts to expand Sanad digital ID coverage to non-Jordanians (e.g., residents and refugees).• Conduct user research to pinpoint challenges of adopting Sanad digital ID at the individual user level, while aiming to improve the activation rate.• Explore the potential to integrate Sanad into the in-person service delivery experience.
Electronic Signature	<ul style="list-style-type: none">• Conduct research and consultations to understand the barriers to the adoption of electronic signatures (including the e-signature application programming interfaces (APIs⁸)).• Explore the addition of lower-assurance-level but higher-usability e-signature solutions in the Sanad application.• Improve the integration of e-signature into the business processes of public- and private-sector service providers.
Public Key Infrastructure	<ul style="list-style-type: none">• Expand the number of accredited certificate authorities (CAs), including private-sector CAs, as well as MDAs that wish to issue digitally verifiable documents and credentials.• Explore additional accrediting registration authorities (RAs) beyond banks, including public- and private-sector institutions.
Consent Management	<ul style="list-style-type: none">• Accelerate the introduction of dynamic consent management mechanisms to improve individuals' control over personal data being shared.• Prioritize user-centric data sharing architectures tailored to the use case to enhance individuals' control over their data.• Promote the adoption of consent-management functionality in the business processes of services operated by line ministries.• Consider the adoption of open standards for consent receipts to promote interoperability and trust, and allow information about the scope and terms of user consent to be shared as metadata with third parties during data sharing transactions.• Raise awareness among data protection implementing authorities about the potential of modern consent management as a key enabler of privacy by design.

3. DATA SHARING

Direct Data Sharing	<ul style="list-style-type: none">• Integrate additional service providers into the Government Service Bus (GSB) and build their capacity to leverage data sharing functionalities to improve their business processes.• Strengthen the GSB audit and transaction logs functionality to improve transparency for users about how the government shares their personal data.• Integrate consent management functionality into the GSB's operations to enable additional data sharing use cases where consent may be a legal basis.
---------------------	---

⁷ SSO is an authentication scheme that allows a user to log in with a single ID to any of several related, yet independent, software systems.

⁸ An application programming interface (API) is an interface that provides programmatic access to service functionality and data within an application or a database. <https://gartner.com/en/information-technology/glossary/application-programming-interface>

Decentralized Data Sharing

- Improve awareness and adoption of verifiable credentials as a data sharing mechanism among the public and service providers and improve the standardization of digitally verifiable credentials issued across government.
- Adopt international standards for verifiable credentials, such as the new World Wide Web Consortium (W3C) standard.⁹
- Develop an implementation plan for service providers to adopt verifiable credentials.
- Establish a trust framework that facilitates mutual recognition of digitally verifiable documents issued across institutions and borders.
- Rearchitect the technical design of the Sanad application to incorporate a digital wallet architecture.¹⁰
- Initiate dialogue with foreign governments around introducing regulations to extend the trust framework across borders.
- Leverage digitally verifiable credentials to improve the implementation of the prime ministerial circular aimed at abolishing the requirement for certification of official documents.
- Improve interoperability between government IT systems to support verification of citizens' data against the authoritative source without requiring issuance of any physical documents.
- Conduct awareness campaigns to educate citizens and relying parties¹¹ about the benefits and procedures of sharing/recognizing digital credentials, which eliminates the need for physical submission and government certification.

Data Aggregation

- Continue to evolve data protection safeguards in line with technological advancements, particularly the adoption of privacy-enhancing techniques, such as data anonymization and tokenization. Include robust checks to reduce the re-identification risk of previously anonymized data, along the lines of data protection legislation and international good practices for data privacy.
- Increase awareness and adoption of the data warehouse by users within the government and explore the potential of deploying artificial intelligence tools to allow government users to better leverage the data contained in the data warehouse.

4. USE CASES

Sanad e-services portal

- Prioritize the digitalization of high-usage services.
- Increase awareness among public- and private-sector service providers about the potential benefits of integrating Sanad microservices into their offerings.
- Enhance Sanad's relevance to private-sector service providers.
- Improve the user experience and user centricity in Sanad platform's design. Incorporate feedback from citizens and best practices from international communities to optimize user experience.
- Assure citizens that their personal data is protected and will only be used for delivering the intended services.

⁹ The emerging international standard for digitally verifiable credentials is the W3C Verifiable Credentials Data Model, currently in version 2.0. <https://www.w3.org/TR/vc-data-model-2.0/>

¹⁰ One notable approach to standardizing digital wallet architectures is the ongoing European Digital Identity Wallet effort. <https://eudiwalletconsortium.org/>

¹¹ A relying party is an entity that relies upon the subscriber's credentials, typically to process a transaction or grant access to information or a system.



2 FOUNDATIONS AND ENABLERS

This diagnostic starts with the identification, computing, and trust foundations for digital transformation in Jordan. Specifically, legal identity, data centers, cloud, and data protection frameworks will be analyzed as components that enable DPI implementation by providing a trusted foundation.

2.1 LEGAL AND REGULATORY FRAMEWORK

Summary

Jordan has made some significant improvements to the legal and regulatory environment needed to ensure inclusive and trusted DPI. Key examples include the development of a legal and regulatory framework that recognizes the validity of electronic transactions and e-signature (2015), the revision of the law on access to information (2024), the adoption of a cybercrime legislation (2023), as well as the long-awaited law on data protection (2023). While these instruments highlight Jordan's commitment to building robust foundations for the country's digital economy, additional legal and regulatory reforms will be needed to fully enable trusted and inclusive DPI in line with international standards. Examples include enacting a legislation that governs the development and implementation of digital ID systems, as well as further strengthening the data protection framework, as highlighted below.

Personal **data protection**, upheld by legal, regulatory, and institutional frameworks, fosters trust by establishing enforceable rights and obligations for the safeguarding of personal data and users' privacy.

The Personal Data Protection Law, enacted in September 2023, incorporates key principles recommended under

international good practice, such as the UN Principles on Personal Data Protection and Privacy and many provisions found in the EU's General Data Protection Regulation (GDPR), including legitimacy of the processing, purpose limitation, accuracy of personal data, and confidentiality. The law also underscores the significance of the data subject's consent and determines the conditions under which such consent justifies the processing of personal data, including specificity, informativeness, expressiveness, and alignment with the purpose. In addition, data subject rights are clearly articulated, and sensitive personal data is distinctly defined and aligns with international good practice.

However, some notable gaps and ambiguities are present in the legislation. Notably, the principle of data minimization (that is, collecting only the personal data necessary for achieving the specific processing purpose) is not explicitly expressed, thus missing an opportunity for a "by-design" and "by-default" approach to data protection. Likewise, the concept of "privacy impact assessments" (PIAs) (also known as "data protection impact assessments"), vital for identifying and managing risks in personal data processing—particularly, in digitalization projects—is not addressed. Despite the lack of a requirement for PIAs at the level of primary legislation, a recent draft implementing regulation¹² mandates the performance of PIAs under certain circumstances to identify and mitigate privacy risks associated with data processing activities, especially those considered high-risk. Article 7 of this draft regulation emphasizes the importance of updating PIAs regularly to ensure accountability and proper documentation. The scope of required PIAs is comprehensive, covering scenarios where sensitive personal data is processed or when activities are conducted on a large scale.

Other weaknesses of the law include the broad nature of some of its exemptions. For example, the Central Bank of

12 Specifically, the decree implementing Article 8(B) of the Data Protection Law, pertaining to internal security and technical organizational measures.

Jordan is allowed to process personal data without the data subject's prior consent and with little limitation. Another such exemption allows for data sharing among public authorities without specifying an alternative legal basis to consent for such sharing, potentially leaving room for the sharing and transferring of personal data without sufficient justification. Finally, the composition of the data protection authority, which includes members from internal security forces, could be seen to raise concerns about the authority's capacity to provide the independent and effective oversight typically anticipated by international standards, potentially undermining trust in the authority and the overall digital government and digital economy.

Recommendations

A future revision to the Personal Data Protection Law or the adoption of secondary legislation, such as implementing decrees, could help address some of the weaknesses identified above. Recommendations include the following:

- Introduce good-practice concepts such as data minimization and privacy impact assessments.
- Reduce the number and scope of exemptions that allow public-sector entities to share and process data without a clear legal basis.
- Improve the independence of the data protection authority and improve alignment of its governance model with international good practice.

2.2 LEGAL IDENTITY

In contrast to digital identity, **legal identity**¹³ (or foundational ID) typically includes civil registration systems, national identification systems, and population registries. Legal ID systems provide recognition before the law and proof of legal identity, offering the necessary proof to establish digital identities and associate them with real-world persons.

Summary

Prior to 2016, Jordanians used a plastic national ID card to comply with the mandatory requirement for citizens to present this form of ID when accessing basic services provided by the government and the private sector. In 2016, Jordan replaced this credential with a new “smart” card that contains an embedded digital chip. Designed to replace the previous plastic card for adults aged 16 years and older, the new national ID card has reached 6.5 million people—over half the country's population. The cumulative coverage of both versions of the national ID card is 97 percent of the eligible population, according to the ID4D 2021 dataset.¹⁴

The new national ID card features several enhancements in security, privacy, and information disclosure. For example, to protect user privacy, the cardholder's religion is no longer printed on the face of the card. The national ID also includes a digital certificate that can be used for signing documents electronically, though its practical application is limited due to the requirement for specialized card reading devices, which come at an additional cost to users and, therefore, are not commonly used for real-world transactions. The low usability of this solution has likely contributed to its low adoption by citizens and relying parties.

Each national ID card holder is uniquely identified using a biometric identification process based primarily on iris biometrics, supported by facial and fingerprint biometric data. The biometric database and accompanying automatic biometric identification system (ABIS) also includes data from additional data sources, such as the registry of residents, whose iris biometrics are captured at border crossings. Overall, this centralized ABIS architecture allows all Jordanian citizens and residents to be reliably and uniquely identified.

For authentication, the smart card's chip can read fingerprint data using a suitable device, which can be used to verify the holder's identity by locally performing a 1:1 match; this is the method that has historically been used for the activation of Sanad accounts. However, with the recent rollout of the iris-based activation process for Sanad accounts (substituting 1:N iris-based identification for fingerprint authentication), there is now an alternative method that allows bypassing the

¹³ A legal identity is the basis on which children can establish a nationality, avoid the risk of statelessness, and seek protection from violence and exploitation. For more information, see *Principles on Identification for Sustainable Development: Toward the Digital Age (English)*. Washington, D.C.: World Bank Group. <http://documents.worldbank.org/curated/en/213581486378184357/Principles-on-Identification-for-Sustainable-Development-Toward-the-Digital-Age>

¹⁴ Clark, Julia Michal; Metz, Anna Zita; Casher, Claire Susan. ID4D Global Dataset 2021: Volume 1 - Global ID Coverage Estimates (English). Washington, D.C.: World Bank Group. <http://documents.worldbank.org/curated/en/099705012232226786/P176341132c1ef0b21ad11abad304425ef>

national ID for Sanad onboarding. This iris-based method is now the dominant onboarding process for most users.

Building on the advancements in Jordan's national ID system, the country has also taken significant steps to ensure the inclusion of refugees within its legal identity framework. Refugees undergo a two-part registration and authentication process. They first update their registration with the UNHCR, which confirms their identity and collects biometric data. They then use the UNHCR certificate to obtain a service card from the Mol, which includes a unique ID number, after a second biometric verification against existing Mol records. Although this process is inclusive, there is potential for it to be streamlined to make the experience more efficient and user-friendly for refugees.

Recommendations

- While the existing national ID card is adequate to facilitate the adoption of DPI, such as Sanad, by Jordanian citizens, there is room to strengthen the credentials used for onboarding non-Jordanians (residents and refugees), military personnel, and potentially even tourists.
- Render Jordan's national ID system (i.e., Mol database) interoperable with UNHCR's systems to simplify the issuance process of service cards for refugees.
- Deploy mobile registration centers to camps and UNHCR registration centers to facilitate large-scale onboarding of refugees onto Sanad.

2.3 DATA CENTERS AND CLOUD COMPUTING

Cloud computing services, and the physical **data centers** underpinning them, are the foundational infrastructure that supports DPI and data-driven innovations. Together, they offer on-demand compute resources over a network, which are critical for the scalability and flexibility necessary for the increasingly data-driven digital transformation of public services.

Summary

Jordan's 2020 Cloud Policy aims to develop a hybrid cloud model, with data hosting requirements tailored to the type of data being hosted. The policy categorizes data into four levels of sensitivity, or risk levels: "secret," "sensitive," "private," and "ordinary," each with specific hosting requirements. The highest risk category, "secret," restricts hosting exclusively to the government's private cloud (GPC)¹⁵ data centers managed by MoDEE, while "sensitive" data must be localized within Jordan but can be on the GPC or a local, private-sector cloud. The two lower-risk categories ("private," "ordinary") drop localization requirements and authorize the use of international cloud providers.

In practice, Jordanian MDAs have been slow to adopt private-sector-provided private clouds, with decisions made on a case-by-case basis by MoDEE. To reduce frictions and promote cloud adoption, MoDEE is working on updated guidelines intended to offer additional options for hosting less-sensitive data, including the adoption of the private-sector, public cloud option.

To illustrate how the Cloud Policy is implemented in practice, the case of Sanad and digital government is instructive. The Sanad application itself is hosted on the Amazon Web Services (AWS) international public cloud, which benefits from reduced latency and optimized data hosting costs, leading to a seamless and responsive user experience. However, the systems responsible for the backend workflows accessible through Sanad, including the GSB and various sectoral databases and applications called by Sanad during service delivery, are hosted on the GPC environment, reflecting the hybrid approach. Sanad is integrated with the GSB through the public Government to Business (G2B) API gateway due to its hosting on a public cloud, i.e., AWS.

Jordan's Cloud Policy envisages a transition period before compliance is achieved across MDAs, allowing time for the migration of legacy systems and for change management. Various timelines are imposed at the policy level, with the overall government migration timeline estimated at five to seven years by MoDEE, even though some MDAs are on track to complete their migration faster. With the current timeline, it is common for MDAs to build new systems and applications in the cloud, while some legacy

15 A private cloud is a cloud infrastructure provisioned for exclusive use by a single organization that comprises multiple consumers (e.g., business units). It may be owned, managed, and operated by the organization, a third party, or some combination of them, and it may exist on or off premises. *For more information, see The NIST Definition of Cloud Computing. National Institute of Standards and Technology. U.S. Department of Commerce. <https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-145.pdf>*

systems continue to reside in sectoral data centers awaiting migration or replacement. MoDEE estimates that between 25 and 40 MDAs have already closed their sectoral data centers entirely after completing their cloud migration.

To ensure compliance with the Cloud Policy and reduce slippage of the migration timeline, there is a general moratorium on upgrading or expanding existing sectoral data centers. On a case-by-case basis, MoDEE has sometimes allowed small upgrades to existing data centers but has refused larger expansion requests. Also, to encourage ministries to migrate to the GPC, MoDEE has at times declined requests to provide technical support to MDAs that still use aging sectoral-level data centers. The shift to cloud adoption has likely been further catalyzed by the fact that GPC's service is provided for free to governmental clients without any cross-sectoral billing (there are nominal fees for the colocation model, where government entities install their own services within the MoDEE data center building.) This "one government" pricing approach means that the costs of GPC are limited to the direct one-time costs of data and system migration, which in many cases comes with cost savings from refreshing and maintaining legacy sectoral data centers.

While military and security services are exempt from the Cloud Policy, some military and security MDAs still use the GPC for specific systems, such as e-services provided directly to citizens over the Internet.

To implement the GPC, MoDEE operates one main data center (DC) and one disaster recovery center (DRC), both located in Amman. Moreover, MoDEE is expanding its infrastructure by leasing colocation space in an existing DC in Aqaba, which would become the third infrastructure node of the GPC. The vision for the GPC architecture includes five DCs, with three highly available DCs in an active-active configuration and two DRCs. The GPC product offering is diverse and tailored to clients' needs, including: (a) infrastructure as a service (IaaS) or managed data centers, (b) database as a service (DBaaS) or managed database services, (c) platform as a service (PaaS) or managed software platforms, and (d) colocation or space for external hardware.

Recommendations

- Conduct stakeholder consultations with MDAs to identify the transitional barriers from legacy systems

and data silos to cloud services. Based on consultation outcomes, implement targeted measures (e.g., data standardization, APIs, migration strategies) to improve Cloud Policy adoption and accelerate the migration to the cloud.

- Continuously refine the Cloud Policy to increase the flexibility of using both national and international public cloud providers for less sensitive data. The move would improve cost efficiency and help develop local cloud markets, while maintaining security, improving service availability and resilience, and increasing alignment with current global technology trends.



3 DIGITAL ID & TRUST SERVICES

This section analyzes Jordan’s digital ID and trust services¹⁶—the core components of the DPI stack that allow people to reliably prove their identities online and service providers to securely authenticate electronic transactions.¹⁷

3.1 DIGITAL IDENTITY

As one of the core components of DPI, **digital identity** is the layer that facilitates digital verification of a person’s identity, including for online transactions. To assure a high level of trust, digital IDs must be linked to a person’s legal identity.

Summary

The Sanad application includes a digital ID functionality primarily used for online service access through the Sanad e-service portal.¹⁸ Authentication involves a username, password, and personal identification number (PIN). An additional facial recognition modality—namely, using a locally stored facial reference image—is planned for future implementation.

While the main use case of the Sanad digital ID is to gain access to services within the Sanad ecosystem, there is also a

federated ID capability. For federated digital ID, MoDEE has published a single sign-on (SSO) application programming interface (API) that is compatible with the internationally recognized OpenID Connect standard¹⁹—an important feature to allow the use of Sanad digital ID for digital service delivery workflows initiated or continued outside the Sanad application. For example, the SSO functionality enables the integration of a “Sign in with Sanad” button on external websites, such as those run by sectoral ministries or private-sector entities. The button redirects users to the Sanad application for ID authentication, and then back to the external website to proceed with their intended tasks. However, this SSO functionality is not widely adopted by MDA service providers.

For in-person service access, the Sanad digital ID is generally not used, as services are typically carried out using the National ID card for Jordanians and an equivalent credential for non-Jordanians. Exceptions include the integration of the Sanad digital ID into the user experience at one of MoDEE-operated Government Service Centers (GSCs)—when booking an appointment, the Sanad application first generates a QR code that can then be scanned by a government agent at a GSC, allowing the service delivery process to proceed. In the future, there may be potential to further integrate Sanad into the in-person service delivery experience.

16 Trust service means 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. For more information, see *UNCITRAL Model Law on the Use and Cross-border Recognition of Identity Management and Trust Services (2022)*, United Nations Commission on International Trade Law. <https://uncitral.un.org/en/mlit>.

17 Electronic transaction means a transaction, action, or set of actions of either a commercial or non-commercial nature that includes the provision of information and/or e-government services. For more information, see *Southern African Development Community (SADC) Model Law on Electronic Transactions & Electronic Commerce, Establishment of Harmonized Policies for the ICT Market in the ACP. Support for Harmonization of ICT Policies in Sub-Saharan Africa (HIPSSA)*. https://www.itu.int/ITU-D/projects/ITU_EC_ACP/hipssa/docs/SA4docs/electronic%20transaction.pdf

18 Digital identity is the unique representation of a subject engaged in an online transaction. A digital identity is always unique in the context of a digital service, but it does not necessarily need to uniquely identify the subject in all contexts. For instance, a person’s digital identity in a healthcare system is used to uniquely access their medical records, but it does not necessarily connect to their driving records, which are irrelevant for medical purposes. For more information, see *Digital Identity Guidelines*. National Institute of Standards and Technology. U.S. Department of Commerce. <https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-63-3.pdf>

19 OpenID Connect is an interoperable authentication protocol based on the OAuth 2.0 framework of specifications. It simplifies the way to verify the identity of users based on the authentication performed by an Authorization Server, and to obtain user profile information in an interoperable and REST-like manner. <https://openid.net/developers/discover-openid-and-openid-connect/>

Figure 2: A woman accesses a public service at a GSC after having booked her appointment online using Sanad



The Sanad digital ID must be activated before it can be used for transactional services. Activation can be done by visiting a Sanad station or post office, meeting an itinerant MoDEE agent, or virtually with a partner bank website or application. Eleven banks currently participate as activation partners, with MoDEE open to expanding participation to additional banks in the future.²⁰ The activation process uses the new national ID card with smart chip capability. To be eligible for activation, a user must have already downloaded the Sanad application and created a basic account. The agent performing the activation uses a card reader device to access the biometric fingerprint data on the smart card chip, and then uses a biometric capture device to perform a match-on-card biometric authentication.²¹ MoDEE recently also rolled out an alternative to the national ID card-based process. It uses iris biometric identification (1:N) against reference images on a central service instead of fingerprint authentication (1:1) against reference images on the card. This new onboarding process—already deployed for national ID card holders—will soon be expanded to non-Jordanian residents, as well as military personnel. A key advantage of developing an onboarding process that is not reliant on the national ID card is that it allows expanding the user base

of the Sanad digital ID beyond Jordanian citizens to other groups, such as non-Jordanian residents and refugees.

Since banks do not have access to the above-mentioned devices and systems, a different process is used when banks carry out the activation of Sanad digital ID, based on their existing Know Your Customer (KYC) data for verification. This process is an artifact of a longstanding practice in Jordan whereby banks legally have a role as “authentication entities.” For example, for in-person transactions, it is common for individuals to ask their bank to write a letter to attest to their identity; this attestation is trusted by virtue of the KYC process the bank has already implemented, allowing a customer to legally access public services. By extending the same logic, the process of activating Sanad with a partner bank can be done entirely online from the bank’s website once the customer has logged in to her bank account, since it can be assumed that an in-person identity verification was already carried out when the bank account was opened. Bank clients whose initial account opening was based on remote onboarding procedures (eKYC) are not eligible for such one-click Sanad activation.²²

20 The number of partner banks reflects the latest count as of August 2024. MoDEE is in the process of expanding its collaboration to encompass more banks in the near future.

21 Biometrics refers to the automated recognition of individuals based on their biological and behavioral characteristics. Ibid.

22 KYC procedures are requirements for financial institutions to verify the identity of the customer and beneficial owner before or while establishing a business relationship or conducting transactions for occasional customers. For more information, see International Standards on Combating Money Laundering and The Financing of Terrorism & Proliferation. Financial Action Task Force. <https://www.fatf-gafi.org/content/dam/fatf-gafi/recommendations/FATF%20Recommendations%202012.pdf.coredownload.inline.pdf>

Despite approximately 3.25 million downloads of the Sanad application, approximately 1.4 million Jordanians have gone through the in-person activation process as of December 2024 (This covers approximately 19 percent of eligible population aged 16 or above).^{23 24} At the time of writing, the activation rate for Sanad was approximately 4,000 accounts per day. Several groups are currently ineligible for activation of the digital ID, namely non-Jordanians (including residents and refugees), military and security personnel, and any undocumented persons. The limitation for military personnel is primarily technical: under Jordanian law, they are not eligible for a national ID card, which was the basis of the Sanad onboarding process until recently.

MoDEE plans to expand eligibility in a multi-phased approach, starting from residents and military and security personnel in the first phase, and then moving on to refugees. For residents, activation will use the same iris biometric identification process that was recently rolled out for citizens, with reference to images being taken from the database captured at border crossings. For refugees, the onboarding process has not yet been defined.

Recommendations

- Carry out consultations with stakeholders, including service providers that rely on Sanad digital ID, to identify and address barriers to adoption of the Sanad digital ID, including of SSO features, and establish methods of integration into their service delivery workflows and business processes.
- Accelerate ongoing efforts to expand Sanad digital ID coverage to non-Jordanians (e.g., residents and refugees), including through innovative adjustments in business processes for Sanad activation.
- Conduct user research to pinpoint the challenges of adopting Sanad digital ID at the individual user level, while aiming to improve the activation rate. The study should assess factors such as usability, perceived relevance, and any specific barriers faced by marginalized groups.
- Explore the potential to integrate Sanad into the in-person service delivery experience. For example, Sanad digital ID could be used for authentication when accessing services using the self-service kiosks that may soon be deployed in the GSCs.

Figure 3: A woman activates her Sanad digital ID at an itinerant MoDEE agent



23 The percentage is based on individuals aged 15 and older, as there is no available breakdown for those specifically aged 16 and above. This means the figure represents a lower-bound estimate of coverage. Source: 2023 population estimates by the Population Statistics Division of the Department of Statistics, Government of Jordan.

24 Individuals aged 16 are eligible to activate the Sanad Digital ID feature. However, since they also need a smart national ID, biometric iris registration, or a bank account—many do not have any of these—the coverage rate remains relatively low. Among those who possess one of the three options, the coverage stands at 37 percent.

Figure 4: Sanad application with digital ID activated



3.2 ELECTRONIC SIGNATURE

An **electronic signature** is a signature generated using digital means for the purposes of authenticating an electronic transaction, designed to enable trust and potentially ensure the same legal equivalence as paper-based signatures.²⁵

Summary

The Sanad application includes an electronic signature functionality, allowing users with activated accounts to generate legally recognized qualified electronic signatures. As part of the activation process of the Sanad digital ID, users also activate an electronic signature account, meaning that every Sanad account holder can create high-assurance qualified signatures. Account activation entails generating a public and private key pair, with the user's private key stored securely in a hardware security module (HSM) in MoDEE's data center.

Jordan's legal framework outlines three levels of assurance for electronic signatures, which correspond roughly to

electronic Identification, Authentication and trust Services (eIDAS) assurance levels: "qualified," "protected," and "normal," with "qualified" offering the highest trust.²⁶ Qualified digital certificates must be issued by either MoDEE, other licensed entities that are accredited as certificate authorities (CAs), or the Central Bank (for financial transactions). The middle ("protected") assurance level is less stringent, requiring only general alignment with asymmetric key technology, without specific infrastructure demands.

The Sanad application is used as a front-end interface for electronic signature generation, with its digital ID functionality ensuring identity verification for e-signature assurance by controlling access to MoDEE's cloud-managed private key used for signing. MoDEE indicates that Sanad's electronic signature feature meets European Telecommunications Standards Institute (ETSI) standards.²⁷ An API interface allows service providers, such as banks, to integrate the e-signature into their own business processes that require signatures, through seamless backend integration with their own systems. This improves usability over a purely application-based workflow and promotes broad e-signature adoption. Despite these capabilities, the adoption of the e-signature API among service providers remains low.

25 For a more in-depth discussion on the role of electronic signatures in fostering trust, see Tullis, Christopher; Constantine, Nay; Cooper, Adam. *Electronic Signatures: Enabling Trusted Digital Transformation*. Digital Transformation Policy Note Series, September 2024. © Washington, DC: World Bank. <https://openknowledge.worldbank.org/entities/publication/d56f94c3-c1c8-4b17-b479-fd68f9551b1c>

26 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. Regulation (EU) 2024/1183 is its latest revision.

27 ETSI is an internationally recognized regional standards body that deals with telecommunications, broadcasting, and other electronic communications networks and services. See standards for electronic signatures https://www.etsi.org/deliver/etsi_en/319100_319199/31912201/01.03.01_60/en_31912201v010301p.pdf

Recommendations

- Conduct research and consultations to understand the barriers to adopting electronic signatures (including the e-signature APIs) by users and relying parties.
- Explore the addition of lower-assurance-level but higher-usability e-signature solutions in the Sanad application to increase adoption among service providers.
- Improve the integration of e-signature into the business processes of public- and private-sector service providers, including through awareness raising and technical assistance.

3.3 PUBLIC KEY INFRASTRUCTURE

A key component of digital trust is **public key infrastructure (PKI)**, which helps provide assurance of data integrity, data provenance, and the security of communication channels. PKI is a key enabler of high-trust electronic signatures and, when implemented as part of a comprehensive trust framework for electronic signatures, can enable digitalization of even the highest-risk transactions.

Summary

Jordan's PKI²⁸ operates on a three-tier model, with a national root certificate authority (CA) serving as the root of trust, a second tier with policy CA servers, and a third tier with multiple issuing CA instances that generate user keys.²⁹ There are various registration authorities, such as the Civil Status and Passport Department of the Ministry of Interior, which is the registration authority (RA) for the digital certificates integrated into the national ID smart card, as well as MoDEE and its bank partners, which serve as RAs in their role in the activation process for the Sanad application. There are separate policy CAs for different types of transactions, including person-to-government (P2G), business-to-government (B2G), and business-to-business (B2B), with the B2B category as its own branch under the national PKI and central bank oversight.

28 PKI is the infrastructure that supports the management of public keys. It provides support to authentication, encryption, integrity, and non-repudiation services. For more information, see *Information technology - Open Systems Interconnection - The Directory: Public-key and attribute certificate frameworks. Recommendation ITU-T X.509. International Telecommunications Union. <https://www.itu.int/ITU-T/recommendations/rec.aspx?rec=X.509>*

29 A certificate authority (CA) is a trusted entity that issues and revokes public key certificates, while a root certificate authority is a CA whose public key serves as the most trusted datum (i.e., the beginning of trust paths) for a security domain. For more information, see *Securing web transactions: TLS server certificate management. National Institute of Standards and Technology. <https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.1800-16.pdf>*

Recommendations

- Expand the number of accredited CAs, including private-sector CAs, as well as MDAs wishing to issue digitally verifiable documents and credentials.
- Explore additional accrediting RAs beyond banks, including public- and private-sector institutions, to increase the accessibility of Sanad and its high-trust e-signature.

3.4 CONSENT MANAGEMENT

In the context of DPI and data sharing, dynamic **consent management** refers to systems, processes, or policies allowing individuals to determine what data they wish to permit various third parties to access, process, or otherwise use. Robust consent management systems should record consent, along with its scope and terms, in a verifiable way while also allowing individuals to dynamically revoke previously provided consent.

Summary

The current version of the Sanad application includes some basic features to record users' consent as part of the e-service request process. For example, some services have an "I agree" checkbox to agree to terms and conditions, which, combined with the authentication needed to access the Sanad application, allows some basic collection of consent for many applications. However, the exact implementation depends on the use case; there is no structured mechanism for ongoing management of consent (including subsequent consent revocation) or for the issuance of a digitally verifiable consent receipt to users.

MoDEE plans to implement a new consent-based data sharing mechanism, which would cover not only user-initiated transactions (such as service requests), but also allow users to provide consent for backend data sharing transactions. Under the proposed architecture, if an entity wants to request a user's data from another entity—for example, through the GSB data sharing platform—it will send a request to the Sanad platform. The platform would then

send a push notification to the user's Sanad application, prompting the user to log in to the application and either give or deny permission for the data to be shared, potentially confirming consent with an electronic signature. Once the consent is given, a consent token will be forwarded back to the requesting party through the Sanad platform, authorizing the data to be shared. The consent management platform would also allow users to update or revoke their consent in Sanad, with accompanying effects on the data-access permissions through the GSB. MoDEE is currently waiting on ministerial approval before moving forward with the implementation of this mechanism.

Recommendations

- Accelerate the introduction of dynamic consent management mechanisms to improve individuals' control over personal data being shared. This could include sending transaction-based consent requests to users of the Sanad application for backend data sharing through the GSB.
- Prioritize user-centric data sharing architectures tailored to the use case to enhance individuals' control over their data and reduce the need for GSB-based data sharing for everyday transactions.
- Promote the adoption of consent-management functionality in the business processes of services operated by line ministries, such as those managing health, education, and social protection programs, or other systems where sensitive personal data may be accessed or processed.
- Consider adoption of open standards for consent receipts to promote interoperability and trust, and allow information about the scope and terms of user consent to be shared as metadata with third parties during data sharing transactions.³⁰
- Work with the authorities responsible for implementing Jordan's data protection legislation to raise awareness about the potential of modern consent management as a key enabler of privacy by design.

³⁰ See for example, International Organization for Standardization, ISO/IEC TS 27560:2023(en) *Privacy technologies – Consent record information structure*. <https://www.iso.org/obp/ui/en/#iso:std:iso-iec:ts:27560:ed-1:v1:en>



4 DATA SHARING

As a core building block of DPI, data sharing is the technical method of getting data from point A to point B, enabling interoperable, open, and inclusive systems for the provision of essential, society-wide, public and private services. Data sharing is carried out in various ways depending on the use case.

4.1 DIRECT DATA SHARING

Direct data sharing involves the integration of two digital systems through an appropriate interface, allowing disparate systems to communicate with each other by defining a set of rules and protocols.

Summary

For MDAs and private entities integrated to the GSB through APIs, real-time data sharing is enabled in transactions at the application level. While such live access to shared data is used mostly for government service delivery, the private sector can also access the GSB through a dedicated API gateway. In general, access to the GSB occurs through one of two API gateways: a private government-to-government (G2G) gateway that is only accessible from the government's private wide-area network (WAN) and a public government-to-business (G2B) gateway that is accessible from the Internet, used for both private-sector integration and for any government services that are hosted outside of the GPC, such as the Sanad application. With the new Personal Data Protection Law in place, further evolution of these systems may be required to ensure compliance, particularly with respect to data governance arrangements, security requirements, authorization and consent policies, transactions logs, and audit capacity.

Recommendations

- Integrate additional service providers, including providers from the private sector, into the GSB and build their capacity to leverage data sharing functionalities to improve their business processes.
- Strengthen the GSB audit and transaction logs functionality to improve transparency for users about how the government shares their personal data, including the entities involved and the purposes.
- Integrate consent management functionality into the GSB's operations to enable additional data sharing use cases where consent may be a legal basis.

4.2 USER-CENTRIC DATA SHARING

User-centric data sharing, also known as decentralized data sharing, allows individuals to share their data directly with verifiers, reducing reliance on databases to be directly integrated to each other while maintaining the benefits of digital verifiability. The approach is user-centric by nature, privacy-enhancing by design, and helps empower data subjects to ensure that their data is shared only with their consent and awareness.

Summary

Official governmental documents, signed by MoDEE and verifiable using a QR code, can be stored, downloaded, exported, and printed in the Sanad application. These digitally verifiable credentials³¹ can then be shared by users directly with relying parties, without requiring data to be shared directly on the backend between two databases. However, the decentralized data sharing ecosystem has not gained

31 This is often manifested as cryptographic proof, such as a digitally signed credential issued under strict rules (e.g., a trust framework).

traction primarily because of issuance (*certificate authority*) and verification (*relying party*) challenges in digital credentials.

On issuance, the decentralized data sharing methodology is currently available only to documents issued by the Sanad platform. Sanad-generated official documents include a digital signature and a QR code for subsequent verification. This dynamic QR code, which features the official electronic seal³² of MoDEE (and is enabled by the MoDEE-managed public key infrastructure), can be verified by any user who has the Sanad app installed. However, due to the centralized nature of the e-seal generation process, documents generated outside of the Sanad portal, such as a paper birth certificate delivered by post, cannot be verified using the Sanad application. This means that apart from MoDEE, all MDAs are unable to directly issue official documents that are digitally verifiable unless they delegate the final issuance and signing to MoDEE.

On verification, the limited privacy-enhancing features in the verification process of credentials is another roadblock that is keeping the decentralized data sharing ecosystem from taking off. While Sanad's verification process includes such features, they are not consistently implemented across document issuers. For example, the process of verifying a paper birth certificate issued by the Ministry of Interior (Mol) raises significant privacy concerns. Each birth certificate features a QR code for verification. When scanned using any standard QR code scanner (such as a phone camera application), it directs to the URL link of an electronic PDF version of the certificate that can be downloaded. Consequently, every issued birth certificate is stored in an unencrypted format on the Mol website, making it openly accessible to anyone who has the link. This is a substantial privacy risk, as millions of individuals' birth certificates are accessible on the open internet without strong access controls. Therefore, harmonizing the verification processes for digital credentials is crucial for improving the interoperability between MoDEE- and non-MoDEE-issued documents, standardizing the issuance and verification workflows, and stimulating the adoption of the decentralized data sharing ecosystem.

Recommendations

- Improve awareness and adoption of verifiable credentials as a data sharing mechanism among the public and service providers and improve the standardization of digitally verifiable credentials issued across government.
- Adopt international standards for verifiable credentials, such as the new W3C standard, with the aim of improving the technical interoperability of the verifiable credentials and their associated QR codes across government.
- Develop an implementation plan for service providers to adopt verifiable credentials, including a capacity building plan for government entities that issue and verify official documents and credentials.
- Enact suitable regulations to establish a trust framework that facilitates mutual recognition of digitally verifiable documents issued by different institutions, and eventually across borders.³³
- When possible, ensure that verifiable credentials are issued through the Sanad application can be signed by the issuing ministries, with the appropriate standardization and trust framework in place.
- Rearchitect the technical design of the Sanad application to incorporate a digital wallet architecture, which could improve interoperability and security, and pave the way to the inclusion of additional documents and credentials from both domestic and international issuers.
- Initiate dialogue with foreign governments around introducing regulations to extend the trust framework across borders, thereby recognizing Jordanian digitally verifiable documents abroad. This dialogue could begin with countries that have large Jordanian diaspora populations.
- Leverage digitally verifiable credentials to improve the implementation of the prime ministerial circular (see Box 1) aimed at abolishing the requirement for certification of official documents (currently done by stamping an official seal onto a paper document)³⁴

32 Electronic seals provide assurance of the origin and integrity of a data message that originates from a legal person. *For more information, see UNCITRAL Model Law on the Use and Cross-border Recognition of Identity Management and Trust Services (2022), United Nations Commission on International Trade Law.* <https://uncitral.un.org/en/mlit>

33 "Trust framework" is a generic term often used to describe a legally enforceable set of specifications, rules, and agreements that govern a multi-party system established for a common purpose, designed for conducting specific types of transactions among a community of participants, and bound by a common set of requirements. *For more information, see Trust Frameworks for Identity Systems. Open Identity Exchange.* <https://openidentityexchange.org/networks/87/item.html?id=175>

34 On August 14, 2023, the Prime Minister (PM) of Jordan issued a circular to all ministries, official departments, institutions, public bodies, public universities, municipalities, the Greater Amman Municipality, and government-owned companies, stipulating that they stop requiring citizens to submit a certified copy of paper documents. The PM requested all entities to inform MoDEE of the necessary technical requirements to enable them to read the data of the original documents shown by the citizen, and to verify their authenticity by linking with the interconnection system. <http://bit.ly/48IK82t>

- that need to be submitted to any governmental entity by citizens.
- Improve interoperability between government IT systems to support verification of citizens' data against the authoritative source without requiring issuance of any physical documents.
- Conduct awareness campaigns to educate citizens and relying parties about the benefits and procedures of sharing/recognizing digital credentials, which eliminates the need for physical submission and government certification.

Figure 5: A selection of official government documents accessible through the Sanad application



Box 1: Jordan's recent efforts to abolish the need for paper-based document certification.

The prime ministerial circular of August 19, 2023 directs all public-sector service providers in Jordan to cease requiring citizens to submit certified paper documents for accessing services. This common practice involves obtaining official stamps to authenticate documents, which the circular aims to replace with digitally verifiable documents. The circular was issued in the context of numerous complaints regarding the unnecessary certification of documents despite citizens presenting original copies. It applies to ministries, official departments, agencies, public universities, municipalities, and government-owned companies. Although the circular instructs service providers to communicate their technical requirements to MoDEE to enable such digital verification, implementation remains limited due to the absence of a robust, interoperable, standards-based system for issuing and verifying official documents.

4.3 DATA AGGREGATION

Pooled data sharing methods, sometimes referred to as data pooling, centralize data to make it easy to access and use by collecting data from different sources and processing or structuring it to facilitate

Summary

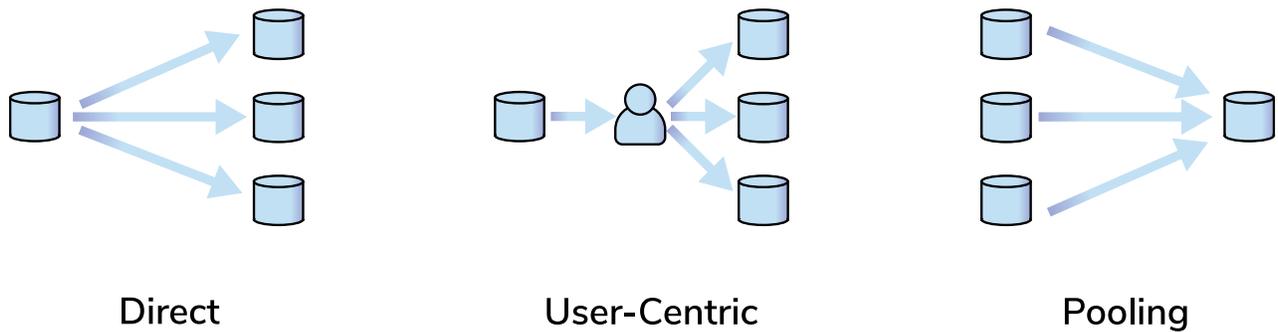
Some MDAs are not integrated with the GSB, due either to security concerns or to a lack of technical readiness for application-layer APIs. In such cases, data may be shared using batch processing, such as extract-transform-load (ETL) or extract-load-transform (ELT), and may be anonymized before being sent to the MoDEE-managed Data Warehouse (DW). The DW acts as a repository for data shared from MDAs, with some policies/protocols in place to govern data updates and retention, varying by data type. The DW's primary

functions are analytics and processing, including for open data, business intelligence, and dashboards. Some, if not all, of the data in the DW is aggregated or anonymized. MoDEE does not share DW data with non-governmental users.

Recommendations

- Continue to evolve data protection safeguards in line with technological advancements, particularly the adoption of privacy-enhancing techniques, such as data anonymization and tokenization. Include robust checks to reduce the re-identification risk of previously anonymized data, along the lines of data protection legislation and international good practices for data privacy.
- Increase awareness and adoption of the data warehouse by users within government. Explore the potential of deploying artificial intelligence tools to allow government users to better leverage the data contained in the data warehouse.

Figure 6: Data Sharing Methods Compared





5 USE CASES

This last section of the diagnostic focuses exclusively on the Sanad platform as a use case for DPI in Jordan. While the integrated e-platform is central to public service delivery in Jordan, the gradual adoption of DPI presents an opportunity to identify further high-impact use cases across sectors for Jordan's evolving digital ecosystem.

5.1 SANAD E-SERVICES PORTAL

As a type of digital service application, **government e-services**—when built on reliable digital foundations and interoperable enablers—supports the front-end delivery of key public services in a user-centric manner. E-services typically come together through an integrated platform designed to provide a suite of public services.

Summary

The *sanad.jo* e-services portal, accessible through the Sanad mobile application installed on a smartphone, contains over 600 digital public services offered by MDAs. At a high level, these services are categorized as either informative (e.g., viewing personal records) or transactional (e.g., applying for governmental services, making bill payments). Some services on Sanad are fully digitalized, meaning that users can handle an entire request through the portal, eliminating the need for an in-person visit to a governmental agency or service center to initiate or complete the transaction. When the service entails the delivery of a document, the user may choose between postal delivery or in-person pick-up. MoDEE plans to increase the number of services that can be completed end-to-end online.

The Sanad application can be downloaded by anyone and offers basic functionality to all users without an account, such as accessing the service catalog and scanning QR codes to verify the authenticity of official documents. To

access a broader range of services—primarily informative—users can create an account through a straightforward, remote process that does not include a rigorous identity check. However, accessing transactional services that may process personal data requires in-person account activation. The latter can be carried out at a Sanad service center or through an official onboarding partner, and it includes a rigorous identity verification process.

MDA service providers can leverage the Sanad platform to enhance the delivery of their services in multiple ways. For instance, (a) Sanad can serve as a one-stop shop where individuals can easily access and initiate service requests. This approach prioritizes ease of access and convenience, catering to simpler and new services needing greater discoverability and/or simplicity. In contrast, (b) providers may choose to integrate specific Sanad microservices, such as digital ID and e-signature, into their service delivery workflows through dedicated APIs. This method is particularly well-suited for established and complex services (e.g., health) with sector-specific workflows, allowing users to start their journey on familiar grounds and leverage the microservices as needed. Additionally, providers can adopt a hybrid approach, offering multiple service entry points to accommodate user preferences and improve accessibility.

Recommendations

- Prioritize the digitalization of additional public services based on usage analytics and user feedback.
- Increase awareness among public- and private-sector service providers about the potential benefits of integrating Sanad microservices into their offerings, regardless of whether the initial service requests are made through the Sanad system.
- Enhance the Sanad platform's relevance to/adoption by private-sector service providers.

- Improve the user experience in Sanad platform's design Incorporate feedback from citizens and best practices from international communities to optimize user experience. Methodologies such as user-centered design can be deployed to approach the issue holistically and inform the design of future versions of Sanad.
- Assure citizens that their personal data is protected and will be used only for delivering the intended services.

Figure 7: A woman browses the available public services using Sanad on her smartphone





6 CONCLUSIONS

Jordan's DPI ecosystem is evolving to support the country's vision to improve digital service delivery. With the core building blocks already in place within a secure and scalable architecture, the focus shifts to increasing service uptake by strengthening interoperability, people centricity, and trust. This diagnostic offers key recommendations to realize these outcomes.

On **interoperability**, this report centers its recommendations on ensuring a seamless identity verification experience for users, across service providers in both the public and private sectors. This is achieved not only through technical enhancements, but also through strategic engagement with these providers. At the technical level, this report recommends enhancing interoperability by standardizing digital credentials across MDAs and aligning them with international standards. Such standardization, gatekept by Jordan's public key infrastructure, ensures that all government-issued documents can be authenticated through the centralized Sanad platform, paving the way for a smoother exchange of data between users and relying parties—a significant step forward in interoperability.

However, technical capability is only one side of the coin. The other side involves encouraging the **adoption of DPI**—such as digital ID, electronic signature, and verifiable official documents—**by the service providers** themselves. To close the gap between technical capability and adoption, it is essential to identify the barriers to adoption by service providers, which will inform the design of solutions to integrate Sanad DPI into their delivery workflows and business processes. The onboarding of additional service providers will directly enhance the interoperability of Jordan's DPI, setting the stage for a more sophisticated data ecosystem which, in turn, elevates digital service delivery across the country.

Moving toward a **people-centric** approach, this diagnostic recommends broadening the use cases of Sanad. By expanding Sanad's DPI functionalities—such as extending

digital ID coverage to non-Jordanian residents and refugees, integrating these services into in-person service delivery, and offering more flexibility in e-signature solutions – Sanad will be well positioned to serve a more diverse user base effectively. To ensure the platform remains relevant and meets the evolving needs of all users, it is crucial to prioritize the addition of new digital services. This should be informed by analyzing user engagement data and incorporating direct user feedback into the development process. To maintain the momentum of Jordan's digital transformation, it is essential to recognize that Sanad is within a larger network of public services. Identifying and actualizing high-impact use throughout different sectors is crucial to harness the rapidly advancing DPI capability of Jordan.

To foster **trust** within the DPI ecosystem, this report underlines the necessity of establishing robust data governance measures. From a governance perspective, future revisions of the Personal Data Protection Law should embed data minimization and privacy impact assessment principles, tighten personal data sharing exemptions, and preserve the independence of the data protection authority. At the Sanad DPI level, this report recommends establishing trust frameworks to enable cross-institutional and cross-border recognition of verifiable credentials. In addition, aligning existing data sharing mechanisms with the new Personal Data Protection Law, along with the introduction of consent mechanisms, would be essential next steps to enhance trust and transparency around the Government's digital transformation efforts.

As Jordan's DPI ecosystem continues to evolve, it will be increasingly important to consider the inherent risk of sidelining vulnerable groups—such as women, refugees, the elderly, and persons with disabilities. A successful DPI hinges on robust systems that prioritize interoperability, people-centricity, and trust, while also ensuring accessibility to leave no one behind.

