A Unified Framework for Secure and Interoperable Digital Identity in South Africa

Sthembile MTHETHWA[1], Sthembile NTSHANGASE[1], Siphelele MYAKA[1], Nomalisa NDHLOVU[1], Samuel LEFOPHANE[1]
[1]*Council for Scientific and Industrial Research (CSIR), 627 Meiring Naude Road, Pretoria, 0001, South Africa*
Tel: +27 12 842 7506, Email: smthethwa@csir.co.za

Abstract: Digital identity represents a technological advancement facilitating the secure access and management of identities for both individuals and organisations within digital environments. Despite considerable progress in digital identity systems over the past decade, their implementation has been hindered by challenges, including fragmentation, lack of interoperability, and inadequate governance framework. This study analyses global digital identity frameworks to identify best practices and opportunities for accelerating adoption, focusing on key principles such as privacy protection, trust, inclusivity, and cross-border interoperability. Additionally, it outlines the essential requirements for a well-governed digital identity ecosystem and proposes a national digital identity framework consistent with international standards, aimed at enhancing the security, resilience, and global recognition digital identities issued in South African.

Keywords: Digital Identity, Digital Identity Framework, Interoperability, Cross-Border Identity, National Identity Frameworks.

1. Introduction

Digital identity has become foundational infrastructure for inclusive digital economies, enabling individuals and organisations to authenticate, authorise, and transact securely across public and private services [1]. Recent estimates indicate that while global progress has been made, approximately 850 million people still lack formal identity credentials, creating barriers to social inclusion and economic participation [2]. South Africa mirrors this challenge through fragmented, non-interoperable identity solutions that impede secure, user centric service delivery [3][4].

South Africa has made important strides, the Smart ID Card and sector specific digital identity technologies are in place, and local innovators have deployed advanced biometric and remote onboarding systems **Error! Reference source not found.**. However, in the absence of a nationally sanctioned, interoperable trust framework aligned to international standards, these initiatives remain siloed **Error! Reference source not found.**. The result is duplication of identity proofing, inconsistent assurance levels, high compliance cost for Know Your Customer (KYC) and SIM registration, limited cross border recognition, and elevated privacy/cybersecurity risks. A coherent trust framework is needed to harmonise assurance, certification, governance, and privacy protections across wallets, issuers, and relying parties, while enabling cross sector and cross border interoperability.

This paper addresses that gap by proposing a South African trust framework for decentralised/self-sovereign identity (SSI). We build on widely adopted specifications (e.g., World Wide Web Consortium (W3C) Decentralised Identifiers (DIDs) and Verifiable Credentials (VCs)) and are informed by leading national and regional frameworks (e.g., ESSIF/EUDI in the EU, Pan Canadian Trust Framework, and the UK Digital Identity and

Attributes Trust Framework). The framework defines ecosystem roles, governance functions, certification requirements for wallets, and conformance mechanisms to protect security and privacy while maximising interoperability. The design is grounded in South Africa's legal context (e.g., National Cybersecurity Policy Framework, National Security Strategy, the Protection of Personal Information Act (POPIA), Cybercrimes Act, Identity Management Policy) and continental efforts toward interoperability led by the African Union [5][6][7].

1.1 Problem Statement

South Africa lacks a unifying, standards-based trust framework for digital identity that specifies common assurance levels, certification processes for wallets, governance roles, and interoperability profiles. In practice, this results in (i) fragmented identity proofing across agencies and industries; (ii) uneven privacy and security controls; (iii) high onboarding friction and compliance cost; and (iv) limited cross border recognition of credentials. A national trust framework is required to align stakeholders on verifiable credential schemas, assurance, certification, and governance, ensuring compliance with privacy law and enabling cross sector portability of identity credentials. (See role/actor needs and governance in the proposed framework section.)

1.2 Objectives

- Define a South African trust framework for SSI, including roles (issuers, holders, verifiers, schema providers, accreditation body, supervisory authority) and their responsibilities.
- Specify security, privacy, and interoperability requirements for digital identity wallets and ecosystem participants, aligned with international standards (e.g., W3C VC/DID, NIST 800 63) and local legislation.
- Describe conformity assessment and certification pathways for wallets (assurance levels, cryptographic requirements, lifecycle management, audit).
- To provide an implementation roadmap with measurable outcomes and Key Performance Indicators KPIs) for government, private sector, and citizens. (KPIs proposed below.)

1.3 Contributions

- A synthesised requirements baseline derived from international frameworks (EU ESSIF/EUDI, PCTF, UK framework, Australia TDIF) and South African legal/regulatory instruments (POPIA, Cybercrimes Act, Identity Management Policy).
- A role-based trust architecture and governance model tailored for South Africa, including accreditation and certification functions.
- Interoperability profiles aligned with W3C DID/VC and AU guidance to support cross border recognition.

The primary research question addressed by this study is as follows:
How can a South African trust framework be formulated to ensure interoperability, security, and privacy within digital identity ecosystems in emerging economies?

The subsequent sections of this document are structured as follows; Section 2 provides a background of existing digital identity frameworks. Section 3 presents a methodology adopted for the study. Section 4 examines the requirements of a Digital Identity Framework. Section 5 explores the proposed digital identity framework and Section 6 concludes this document.

2. Background

Digital identity frameworks have been proposed on an international scale by countries at the forefront of the digital identity sector. Specifically, eight members of the Digital Identity Working Group, which include Australia, Canada, Israel, New Zealand, Singapore, and European nations such as Finland, the Netherlands, and the United Kingdom, have advanced these propositions [8].

In 2022, the SSI Framework for the Web (SSI4Web) was introduced. It integrates SSI principles into web services to enhance security, user autonomy, and flexibility [9]. The framework is compatible with web services that adhere to specified protocols and data formats, such as W3C, VCs and DIDs. It employs cryptographic keys for secure authentication, thereby eliminating the necessity for conventional passwords.

In Canada, the Pan-Canadian Trust Framework (PCTF) is designed to establish trust in services and networks (DIACC, 2023). Moreover, the Canadian digital identity ecosystem was developed to include an integrated authentication and intermediary licensing model, which encompasses individuals, organisations, systems, or authoritative institutions [10].

In Europe, the introduction of the European Self-Sovereign Identity Framework (ESSIF) has been established to integrate digital identity ecosystems into existing regulatory frameworks [11]. The framework delineates the objectives of the EU Digital Identity Wallet, roles of DID ecosystem actors, and outlines both functional and non-functional requirements of the wallet, ensuring compliance with applicable standards, frameworks, legislations and issues pertaining to security, privacy, and trust.

The EU's DID framework is being adopted by several countries, including Finland, the Netherlands, the UK, and Israel. Finland is actively working towards the development of self-sovereign identity frameworks, whereas the Netherlands is participating in the electronic identification and trust services regulation, known as eIDAS **Error! Reference source not found.**. Recent enhancements to this regulation has led to the creation of the EUDI-Wallet. The UK's digital identity and attributes trust framework is focused on ensuring inclusivity in products and services, as well as upholding privacy, data protection, fraud management, and security. Meanwhile, Israel is proposing a system that aligns with ISO standards and is exploring compatibility with eIDAS standards. Singapore, lacking specific legislation dedicated to National Digital Identity, relies on related legal Acts to construct a DID framework, which includes the Public Sector (Governance) Act, the Personal Data Protection Act, the Banking Act and Insurance Act, the National Registration Act, and the Electronic Transactions Act (World Bank, 2022).

The African Union (AU) has formulated a draft for an Interoperable Digital ID Framework for Africa [13]. This framework proposes various models of identity credentials, such as digitally signed credentials and digital wallets, aimed at empowering citizens by granting them control over their personal data, while simultaneously ensuring privacy and security. Nigeria has introduced the Open Standards Identity API (OSIA) digital identity framework, which consists of an open standard set of interfaces designed to enable seamless connectivity within the identity management ecosystem.

The frameworks identified in this research illustrate that Africa remains behind in the field of digital identities. As more nations engage with the digital identity frameworks, it is anticipated that this will lead to the development of additional frameworks, particularly within African nations. This document seeks to address this challenge by proposing a South African-based framework. To ensure effective cross-border systems, it is essential that the frameworks are capable of intercommunication, facilitating seamless integration across various countries without encountering legal or technical impediments. Consequently, the following section presents the methodology adopted for this work.

3. Methodology

The main objective of this research is to propose a Trust Decentralised Identity (DID) Framework specifically tailored for the South African context. To achieve this, the study adopts a four-phased qualitative research design that synthesises international standards, regional strategies, and local legislative requirements.

3.1. Phase 1: Jurisdictional and policy review (requirements identification)

The first phase involves a comprehensive documentary analysis of the primary drivers for digital identity. This phase identifies the boundary conditions for the proposed framework. Regional alignment includes the analysis of the AU interoperability Framework for Digital ID to ensure cross-border compatibility within the African Continental Free Trade Area (AfCFTA). In addition, the national policy context includes the review of the Draft Official Identity Management Policy (2020), the National Cybersecurity Policy Framework (NCPF), and the National Data and Cloud Policy (2024) to align with South Africa's digital transformation roadmap.

Phase 2: Technical and security benchmarking

In this phase, we map international technical standards against the functional requirements of a DID system. For security controls, we have utilized the NIST Cybersecurity Framework (CSF) and the ISO/IEC 27000 series to define the security architecture required for decentralised trust. Operational Integrity, integrating the Cybercrimes Act 19 of 2020, to ensure the framework provides legal recourse for identity-related offenses and unauthorized data access.

Phase 3: Regulatory compliance and data governance

This phase focuses on the Privacy by Design aspect of the Trust DID framework. It includes privacy alignment, a rigorous mapping of POPIA, specifically accountability, processing limitation, and security safeguards, to the decentralised data storage model. In addition, sectoral standards, reviewing the SIMS (Standard for Information Security Management), to ensure the framework meets specific governmental and institutional security mandates in South Africa.

Phase 4: Framework synthesis and validation

The final phase employs Conceptual Framework Development (CFD) to integrate the findings into the Trust DID Framework. This includes thematic synthesis, applying Affinity Mapping to group requirements into three pillars: Governance, Technical Security, and User Sovereignty. In addition, internal validation, the proposed framework is stress-tested against the MECE (Mutually Exclusive, Collectively Exhaustive) principle to ensure no regulatory gaps exist and that the proposed DID model does not conflict with existing South African laws.

4. Requirements for a Digital Identity Framework

The establishing of clear and comprehensive requirements is a prerequisite for the successful functioning of a digital identity framework. These requirements must ensure alignment with strategic objectives, mitigate risks, prioritise user needs, and promote interoperability, scalability, and regulatory compliance. Additionally, they facilitate stakeholder understanding, enhance user satisfaction, and uphold industry standards and emerging regulations. The following categories outline the key requirements for a robust digital identity system:

- Legal requirements - are defined by national and international regulations. In the South African context, these include certification protocols for digital identity wallets to ensure compliance with functional, security, and privacy standards. Such certification promotes interoperability, trustworthiness, and a high level of security across systems.
- Regulatory requirements - these encompass South Africa's digital identity regulations, strategies, and legislative frameworks. They include national acts and programmes that govern the implementation and operation of digital identity systems, ensuring alignment with public sector mandates and digital transformation goals.
- Functional requirements - specify the capabilities of the digital identity wallet. These include the provisioning and management of identity attributes, secure authentication mechanisms, lifecycle management, and support for federated identity models. The wallet must enable users to interact with digital services securely and efficiently, while maintaining privacy and control over their personal data.

Given that digital identity systems rely on storing and protecting personal data, robust safeguards must be implemented to ensure data protection and privacy. Inadequate measures or safeguards can lead to data breaches, resulting in theft or unintended data loss. Therefore, adherence to data protection and privacy legislation and international best practices is essential to prevent theft or accidental data loss. Table 1 outlines some of the legislations that must be considered for all South African digital identity systems.

Name	**Description**	**Relevance**
Cybercrimes Bill & Act	With cybercrime on the rise, threatening data and security, this Act unifies laws to combat criminals, terrorists, and hostile states. Applicable to all computer users and those in ICT, data protection, and regulatory compliance.	Digital identity systems must comply with the legislation to avoid penalties. Given the sensitivity of stored data, proactive measures against cyberattacks are crucial.
The Protection of Personal Information Act (POPIA)	Modelled on the GDPR, POPIA governs how organisations handle personal data in South Africa, regulating data collection, use, and storage under strict legal guidelines.	As digital identity systems process sensitive data such as biometrics, POPIA compliance is essential for trust and liability reduction. Systems must support data subject rights, embed privacy by design, and ensure secure cross-border transfers.
Identity Management Policy	Issued by the Department of Home Affairs (DHA), the policy embraces digital identities from the Fourth Industrial Revolution (4IR) and addresses the need for data security against cyber threats.	South Africa's digital identity framework ensures a secure, inclusive National Identity System, setting standards for creating, verifying, and managing digital identities in alignment with constitutional rights and privacy laws, enhancing service delivery and reducing fraud.
AU Interoperability Framework for	This framework proposes a unified method for individuals to share verified digital identity claims with service	The framework is crucial for South Africa's alignment with Africa's digital future,

Digital ID	providers, establishing common standards for legal identity in digital format relevant to SA as an AU member.	focusing on interoperability.
The NIST Special Publication 800-63-3	It provides technical requirements for implementing digital identity services, ensuring privacy, security, and interoperability for digital identity systems.	Focused on risk-based identity management, strong authentication, and privacy. Originally for U.S. federal systems, supports secure e-government and fraud prevention in South Africa. Aligning with NIST fosters interoperability and trust.

Taking these requirements and regulatory considerations into account, we can define a proposed framework that fully reflects them. Enabling a robust and interoperable solution for the country. The detailed design of this framework is presented below.

5. Proposed Trust DID Framework

The proposed framework seeks to eliminate dependence on fragmented digital identity systems by facilitating South African innovators' adherence to a nationally sanctioned standard. This initiative addresses challenges associated with isolated, unsecured, and unrecognised systems, thereby bolstering security and resilience across all platforms. By implementing a unified framework, the country can maintain control over the entities authorised to issue and verify digital identities, thus ensuring that identities issued in South Africa gain recognition beyond national borders, promoting cross-border interactions and augment interoperability. Achieving this objective necessitates the examination of global best practices and the alignment of the framework with internationally accepted standards. The proposed framework, as depicted in Figure 1, delineates several roles tasked with executing specific security requirements. The proposed framework is aimed at eradicating reliance on fragmented and unregulated digital identity systems in South Africa.

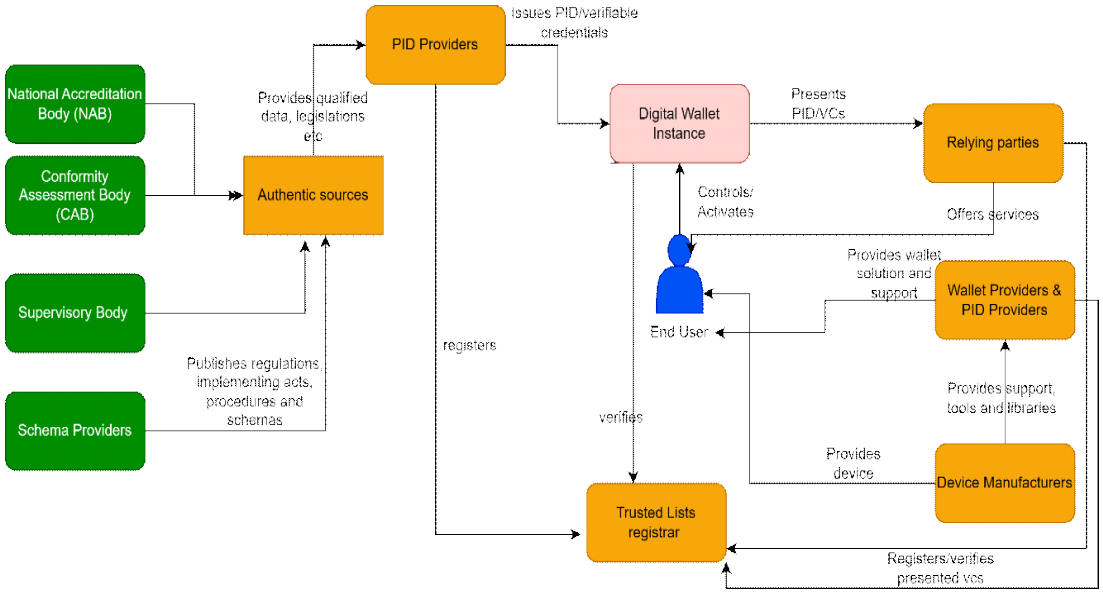

Figure 1: Proposed Digital Identity Framework.

To ensure the effective functioning of the proposed framework, it is necessary to delineate the following roles and responsibilities:

- Authentic Sources - these are public or private repositories or legally mandated systems that contain attributes pertaining to natural and/or legal persons, such as licenses, educational qualifications, public permits, and addresses. These sources must provide interfaces to verify the authenticity of such attributes, either directly or through an intermediary recognised at the national level.
- Administering Authority/Supervisory Bodies - these entities are responsible for governing the framework, reviewing compliance, and ensuring proper functioning of wallet providers and other relevant actors. They must be established and appointed within the jurisdiction of South Africa.
- Conformity Assessment Bodies (CAB) – these are accredited public or private entities, authorised by South Africa's national accreditation body, tasked with certifying and regularly auditing digital wallets.
- National Accreditation Body (NAB) - is the national authority responsible for accrediting CABs that evaluate qualified trust and schema providers.
- Schema Providers – these entities publish schemas and vocabularies that define structures and semantics for digital identity credentials. Such schemas enable entities like relying parties to discover and validate credentials. Common schemas are essential for widespread adoption.
- Trust Anchors/Person Identification Data (PID) Providers – these are trusted issuers of verifiable credentials, such as official identity documents. They may also serve as wallet providers.
- End Users/Holders – these are individuals who utilise digital identity wallets to receive, store, and present verifiable credentials, thereby proving their identity.
- Trusted Lists Registrar – this entity maintains and publishes a trusted list of recognised entities, including wallet providers and PID issuers, complying with national legislation and framework requirements.
- Relying Parties/Verifiers – these entities request necessary attributes from users for verification and maintain an interface with the digital identity wallet to request attestations with mutual authentication. They also authenticate PIDs or verifiable credentials.
- Device Manufacturers and Subsystem Providers – these entities play a crucial role in enabling wallet solutions to function securely and efficiently for end users. They provide platforms (hardware, operating systems, secure cryptographic modules, libraries, app stores) that ensure usability, security, stability, and connectivity.
- Wallet Providers – these are organisations mandated or recognised by South Africa to provide wallets to end users in compliance with the requirements for a digital identity framework.
- Digital Wallet Instance – a digital identity wallet used by end users.

The establishment of these roles ensures clarity in governance structures and accountability among all participants within the digital identity ecosystem. By defining responsibilities at every level, from authentic sources to wallet providers and supervisory bodies, the framework fosters trust, security, and interoperability. By assigning clear authority to governance bodies such as CABs, NAB, and trusted list registrars. The framework supports regulatory compliance by ensuring that all the roles are governed accordingly and ensures that identity credentials can be trusted across jurisdictions. Collectively, these roles form the foundation of an integrated framework that supports national objectives while also

aligning with international standards. With these roles defined, components of a trust DID framework are defined below.

5.1 Components of the trust DID Framework

This section presents the key components of a digital identity framework that include interoperability, security, and privacy in digital identity ecosystems.

Interoperability
A robust framework should promote digital identity awareness among stakeholders, implement advanced security measures like biometric authentication and multi-factor authentication, and integrate digital identity solutions with other technologies like Internet of Things (IoT) devices for secure interactions [14]. Additionally, standards for interoperability, security, and privacy in digital identity systems should be developed and adopted, and compliance with privacy regulations should be ensured. As service delivery becomes increasingly digital, individuals, governments, businesses, and other organisations must trust the accuracy and integrity of the information or identities shared with them. The frameworks aim to enable cross-border systems that do not work in isolation but can communicate seamlessly, making it easier to incorporate various countries' systems without infringement [8].

Security
The security dimension of the framework must include enrolment and identity proofing, digital authentication and lifecycle management, and federated identity management provides requirements for federated identity, and address governance principles for developing the DID ecosystem, related to required administration, identity management, authorisation, access, and authentication [16]. The framework must emphasise robust security measures to protect sensitive information and maintain trust in digital identity systems, including protection against data breaches, identity theft, and unauthorised access [9]. Further, security frameworks must embed roles such as governance authority to ensure oversight and compliance.

Privacy
Privacy protection is integral to maintaining trust in digital identity systems. The framework must ensure compliance with privacy legislation including GDPR, HIPAA, and POPIA, while preventing data breaches, identity theft, and unauthorised access. Privacy-by-design principles should be incorporated into system architecture, ensuring that privacy measures are embedded from inception [10]. Furthermore, it ensures compliance with privacy legislation to uphold user rights and prevent misuse of information.

Upon proposing a framework, it is crucial to make recommendations as to how it might be implemented and a high-level roadmap and the section below aims to achieve that.

5.2 Recommendations and Roadmap

The overarching objective of the proposed framework is to eliminate fragmented, unregulated digital identity systems in South Africa and replace with a secure, cohesive and nationally governed framework for how digital identity systems in South Africa are issued and use and this should be aligned with global standards to ensure cross border compliance. To ensure a successful implementation of this framework, it is crucial for organisations from both public and private sector to work hand in hand and eliminate silos. To govern

this, a Digital Identity council or committee may be established that reports directly to the President, consisting of representatives from various sectors.

To operationalise the Framework depicted in Figure 1, a phased roadmap is recommended. This ensures controlled rollout, stakeholder readiness and early establishment of trust. These are as follows:

- Phase 1 – Foundation and Governance (0 - 4 months): which lays the groundwork for a trustworthy, standards-aligned ecosystem. Achieved through designating roles like the NAB, CABs, the Supervisory Body, and Schema Providers, and issues the core regulatory instruments and technical schemas that will govern participation. The result here, includes having the governance model in place.
- Phase 2 – Standards and Ecosystem Design (4 - 6 months): during this period, the roles defined in phase one are responsible for establishing minimum requirements for PID Providers and Wallet Providers are published. A basic, publicly accessible Trusted Lists Registrar is created to host accreditation status, keys, and revocation information. The result is a clear governance model, a reference architecture, and trust requirements that set expectations for all actors before any credential issuance begins.
- Phase 3 – Pilot Implementation (6 - 12 months): validates the framework through controlled, end-to-end pilots. A small cohort of PID Providers and Wallet Providers is accredited under the draft criteria, and integrations are established with at least one authoritative source. Test users receive pilot PID/Verifiable Credentials, and relying parties from priority sectors exercise issuance, storage, presentation, and verification flows under realistic load. Device Manufacturers collaborate to validate secure key storage and wallet/device binding, while the Supervisory Body oversees privacy, security, and testing. Findings are captured in a pilot evaluation report, informing refinements to procedures, schemas, and security controls ahead of national scale-up.
- Phase 4 – National Rollout (12 - 24 months): With lessons incorporated from the previous phase, the program expands to full production. Accreditation opens to all qualified PID and Wallet Providers, and major public and private relying parties (banking, telecoms, healthcare, education, government services, etc) are onboarded using standardised toolkits and conformance tests. Public awareness and onboarding support are scaled, while continuous interoperability testing ensures a smooth multi-provider environment. By the end of this phase, the digital wallet and verification services are widely available and stable.
- Phase 5 – Optimisation, Cross Border Interoperability and Continuous Compliance (24+ months): the final phase focuses on resilience, expansion, and long-term trust. Providers undergo periodic re-certification and risk-based audits, while the Supervisory Body monitors operational metrics, incident response, and user protection outcomes. The framework aligns with international standards and trust schemes to enable cross-border recognition, and advanced privacy-preserving features, such as selective disclosure, zero-knowledge proofs, etc., are progressively adopted. The ecosystem remains adaptive, secure, and user-centric as new threats, technologies, and use cases emerge.

This phased implementation roadmap provides a clear, pathway for operationalising the Framework in a controlled, secure, and scalable manner. The roadmap ensures that each stage builds confidence, addresses risks early, and strengthens ecosystem readiness. this approach establishes a solid foundation for a trustworthy, user-centric, and resilient digital identity ecosystem that can evolve sustainably as new standards, technologies, and cross-border opportunities emerge.

6. Conclusions

The advent of digitisation has significantly advanced the proliferation of digital identities, as evidenced by the establishment of numerous digital identity systems. Technology plays a pivotal role in the effectiveness of these systems. The transition from traditional, centralised digital identity systems to SSI-based systems provides remarkable opportunities for identity holders to exercise control over their identities. Nonetheless, this transition necessitates the implementation of appropriate framework to ensure that the development and administration of these systems adhere to specified standards. Consequently, the development of the framework is fundamental to informing the development of digital identity.

This article seeks to understand the current digital identity frameworks implemented by various nations. Furthermore, it delineates the requirements for effectively governed digital identity systems and their expected operational modalities to assist the framework definition. Legislative frameworks and regulatory standards significantly influence the management of digital identity systems, particularly regarding the goals to achieve cross-border and interoperability, and these are explored.

The primary objective of this framework for a digital identity system is to restore trust when using the system, allowing identity owners, organisations, businesses, etc, to carry out their activities securely and provide a protective regulatory framework for all involved stakeholders. This is achieved while ensuring data protection and privacy by adhering to relevant legislation and striving for an interoperable system that can operate across borders. Accordingly, this document proposes a digital identity framework for South Africa. The framework detailed the roles and responsibilities for each participant in the framework. The authors intend for this article to serve as a resource for organisations, policymakers, system designers, and developers, supporting informed decision-making in the design and implementation of digital identity systems. To assist with the operationalisation of the proposed framework, the paper proposes a high-level phased approach that is future looking.

Future research will incorporate a detailed technical assessment of system architecture, integration pathways with existing national infrastructure, scalability requirements, cost modelling, and operational feasibility to strengthen the practical implementation case. Additionally, it will involve developing a quantified business case, including economic impact estimates, sustainability considerations, and clearly defined stakeholder incentives, would provide an evidence-based foundation to support national adoption of the proposed framework.

Acknowledgements

Declaration of use of content generated by Artificial Intelligence (AI) (including but not limited to Generative-AI) in the paper

References

[1] Masiero, S., & Bailur, S. (2021). *Digital identity for development: The quest for justice and a research agenda*. Information Technology for Development, 27(1), 1–12. https://doi.org/10.1080/02681102.2021.1859669.

[2] Clark, J., Diofasi, A., & Casher, C. (2023). 850 million people globally don't have ID-why this matters and what we can do about it. World Bank Blogs. Retrieved from https://blogs.worldbank.org/digital-development/850-million-people-globally-dont-have-id-why-matters-and-what-we- can-do-about.

[3] Beduschi, A. (2021). *Rethinking digital identity for post-COVID-19 societies: Data privacy and human rights considerations*. Data & Policy, 3(e15). https://doi.org/10.1017/dap.2021.15.
[4] Sedlmeir, J., Smethurst, R., Rieger, A., & Fridgen, G. (2021). Digital identities and verifiable credentials. Business & Information Systems Engineering, 63, 603–613. https://doi.org/10.1007/s12599-021-00722-y [link.springer.com]
[5] Schardong, F., & Custódio, R. (2022). Self-Sovereign Identity: A Systematic Review, Mapping and Taxonomy. Sensors, 22(5641). https://doi.org/10.3390/s22155641 [researchgate.net]
[6] Open Identity Exchange (2022). Trust Frameworks for Smart Digital ID. https://openidentityexchange.org/files/user_assets/533.pdf [openidenti...change.org]
[7] Gómez, S. (2025). Trust Models for Digital Identity: State of Play. Blockstand Report. https://blockstand.eu/... cite turn1search7
[8] Ntshangase, S., Lefophane, S., Singano, T., Shadung, D., Mokoena, N., & Mthethwa, S. (2023, November). Digital identity frameworks: a review. In International Conference on e-Infrastructure and e-Services for Developing Countries (pp. 3-18). Cham: Springer Nature Switzerland.
[9] Ferdous, M. S., Ionita, A., & Prinz, W. (2022). SSI4Web: A Self-sovereign Identity (SSI) Framework for the Web. International Congress on Blockchain and Applications. Cham: Springer International Publishing.
[10] Rasouli, H., Valmohammadi, C., Azad, N., & Abbaspour Esfeden, G. (2021). Proposing a digital identity management framework: A mixed-method approach. Concurrency and Computation: Practice and Experience, 33(17), 62-71.
[11] Du Seuil, D. (2019). European Self Sovereign identity framework
[12] The World Bank. (2019, August). Inclusive and trusted digital ID can unlock opportunities for the world's most vulnerable. World Bank, Who We Are, News. Retrieved from https://www.worldbank.org/en/news/immersive-story/2019/08/14/inclusive-and-trusted-digital-id-can-unlock- opportunities-for-the-worlds-most-vulnerable
[13] Grassi, P., Garcia, M., & Fenton, J. (2020). Digital identity guidelines (No. NIST Special Publication (SP) 800-63-3). National Institute of Standards and Technology
[14] Jing, Y., Li, J., Wang, Y., & Li, H. (2021). The Introduction of Digital Identity Evolution and the Industry of Decentralized Identity. 2021 3rd International Academic Exchange Conference on Science and Technology Innovation (IAECST), 504- 508. https://doi.org/10.1109/IAECST54258.2021.9695553.
[15] Preukschat, A., & Reed, D. (2021). Self-sovereign identity. Manning Publications.
[16] Imprivata. (2023). Digital identity framework. Retrieved from https://www.imprivata.com/digital-identity-framework