Digital Identity Frameworks: A Review

Sthembile Ntshangase(✉), Samuel Lefophane, Tanita Singano, Daniel Shadung, Nthabiseng Mokoena, and Sthembile Mthethwa

Information and Cyber Security Centre (ICSC), Council for Scientific and Industrial Research, Pretoria, South Africa
{sntshangase,slefophane,tsingano,dshadung4,nmokoena, smthethwa}@csir.co.za

Abstract. Government organisations from various countries worldwide including the South African government, are working towards employing digital identity to solve identity challenges such as, identity theft, individuals lacking identity etc. The use of digital identity has demonstrated promising outcomes to overcome these challenges while maintaining security and privacy of individuals. However, it is crucial to use appropriate governance frameworks to ensure proper handling and issuance of digital identities. Hence, this paper presents a review conducted to determine and understand various frameworks that have been proposed and implemented by other countries. This review contributes by guiding South African organisations, researchers, and decision makers towards understanding which frameworks are currently being used and which framework/s can be considered when developing a South African based governance framework that will ensure interoperability in digital identity systems.

Keywords: Digital Identity · Governance Frameworks · Security · Trust · Privacy

1 Introduction

The issue of identity has been prevalent for a long time and according to the World Bank (2016) 1.5 billion people cannot, at the time of the report, prove their identity [1]. This study was recently updated, and at the end of 2022 the statistics indicated that under 850 million people around the world do not have an official identity (ID) [2]. This invisibility has significant implications for a range of development outcomes that depend on delivering services to people or on them being able to access services. Identity plays a huge role by allowing individuals to exercise their rights and responsibilities fairly and equally in a modern society [3]. Identity is crucial to social inclusivity whereby individuals can now access essential services. In the past, identity has been in physical formats, however, with the rise of the Internet and the Fourth Industrial Revolution (4IR) characterised by digitisation has ushered in a new era of "*digital identities*" [4]. This was further exacerbated by the COVID-19 pandemic, where individuals and organisations were forced to adapt to new ways of conducting business.

A. Sere et al. (Eds.): AFRICOMM 2023, LNICST 587, pp. 3–18, 2025.
https://doi.org/10.1007/978-3-031-81570-6_1

Presently, with billions of globally connected devices such as, computers, smartphones, cameras, supermarket scanners, payment systems, etc.; petabytes of data are now generated and consumed hourly to provide services. Technology is ingrained in even the smallest of devices and is connecting everything, making it a part of our daily life [5]. When making use of services offered by the evolving technology, one option for authenticating, identifying, and verifying a person is to use digital identity. Digital identity is the transformation of physical identities into a digital format to enable three functions, namely the digital identification of individuals, their authentication at various access points, and their authorisation to perform specific actions or access specific services [3]. These functions are critical for a digital identity model to reach its full potential and demonstrate its benefits. The following presents some of the benefits of digital identities that include:

- Privacy Protection: Mobile solutions can allow users to control, share, and easily authenticate their credentials to access various online services. This lessens the chance of unwanted information exchange and data breaches.
- Global Identity Trust: Individual's credentials can be instantly verified, regardless of geographical location or cross-border limitations, through the establishment of universal digital identity framework of trust.
- Smart City Access: Digital identity can be used to increase engagements (with government, public and private organisations) and efficiency in accessing smart cities.
- Inclusive Growth: It can increase economic growth by reducing the number of people worldwide who are excluded in financial and governmental services due to lack of identity documents that can be proven.
- Interoperability: Users can share their digital identities across various platforms, services, and organisations without being tied to a specific identity provider. This eliminates the need for multiple accounts by enabling consumers to access various online services with a single digital identity.
- Customer Trust & Regulatory Compliance: The use of digital identity contributes towards improving organisations Know Your Customer (KYC) strategy and provides efficient customer onboarding, reducing manual verification processes and ensuring compliance with the requirements for regulation.

Even though a digital identity is required for a wide variety of services some are online, and some are physical, there is no "one-size-fits-all" approach towards implementing IDs and access systems [6]. While an increasing amount of personal and critical business information is collected and available online, provisions must be made to ensure security of sensitive data. There is a growing movement among government bodies for the adoption of a digital identity framework that allows users to provide alternative forms of IDs to access key services. This requires creating a digital identity framework to complement and/or act as an alternative to physical documents such as passports or ID cards [7].

Thus, as the South African government is also in a process of adopting digital identity for their services, it is vital to ensure that they adjust to the new era and are not left behind in these new developments. This paper presents the review conducted to determine existing digital identity frameworks, and the major components in those frameworks that can assist South African government towards developing a secure and universal

digital identity system. The remainder of this paper is organised as follows. In Sect. 2 an overview and different models of digital identities is provided. Section 3 presents work done towards developing digital identity frameworks. Section 4 summarises identified digital identity frameworks, and discussions. Finally, in Sect. 5 conclusions are drawn and future directions are presented.

2 Overview of Digital Identities

Digital identity has been defined in various ways, but according to the International Telecommunication Union (ITU) digital identity is defined as a "representation of an entity in the form of one or more attributes that allow the entity or entities to be sufficiently distinguished within context" [8]. The Australian Digital Transformation Agency refers to it as "safe, secure and convenient way to prove who you are online, to access online services" [5]. In THALES view, it is "a set of validated digital attributes and credentials for the digital world, similar to a person's identity for the real world" [9]. Based on the National Institute of Standards and Technology (NIST), it is the "unique representation of a subject engaged in an online transaction." They further clarify that; a digital identity is always unique in the context of a digital service but does not necessarily need to uniquely identify the subject in all contexts [3]. This may mean that "accessing a digital service may not mean that the subject's real-life identity is known" which presents another aspect for digital identities [9]. All these definitions are almost the same, however, other aspects are introduced like the uniqueness introduced by NIST. In our view, digital identity can be defined as a unique and/or detailed digital representation of a subject in a form of attributes and credentials for digital services/context.

2.1 Digital Identity Ecosystems/Architecture Models

Digital identities have evolved tremendously over the past few years. The fist model being a *centralised model* whereby a single *entity* establishes and manages identities in a centralised storage [3]. This model forces users to be dependent on the organisation that holds their data. This approach also centralises cyber risks making it easier for cyber attackers to succeed as they are only required to attack one central point. Regardless, this model is still widely used due to its simplicity and convenience.

To address some of the issues presented by centralised models, a *federated model* was introduced which consists of a group of organisations that have established trust amongst each other. In the group, one organisation becomes the main player known as the Identity Provider (IDP), which holds the user's data. The user can access services offered by other organisations in the group through the IDP, thus introducing the concept of Single Sign-on (SSO). This approach introduces power aggregation whereby more power resides with the IDP; hence, it becomes vulnerable to single point of failure.

Data silos are the main challenge with the previous models. As a solution a *decentralised model* was introduced with the aim of removing silos and IDP's and move towards a user centric approach (where users have full control over their data). Consequently, introducing the concept of *Self-Sovereign Identity (SSI).* This model is still in its initial stages and still requires efforts towards establishing its governance model.

Therefore, this research aims to study some of the governance models, frameworks or policies that have been established in other countries and propose a framework/s that would be ideal when developing a South African based framework. This is crucial for a successful implementation of a digital identity ecosystem.

2.2 South Africa's Digital Identity Roadmap

Just like any other country, South Africa's journey has evolved and with that implementation of various digital identity programs was experienced as depicted in Fig. 1 below.

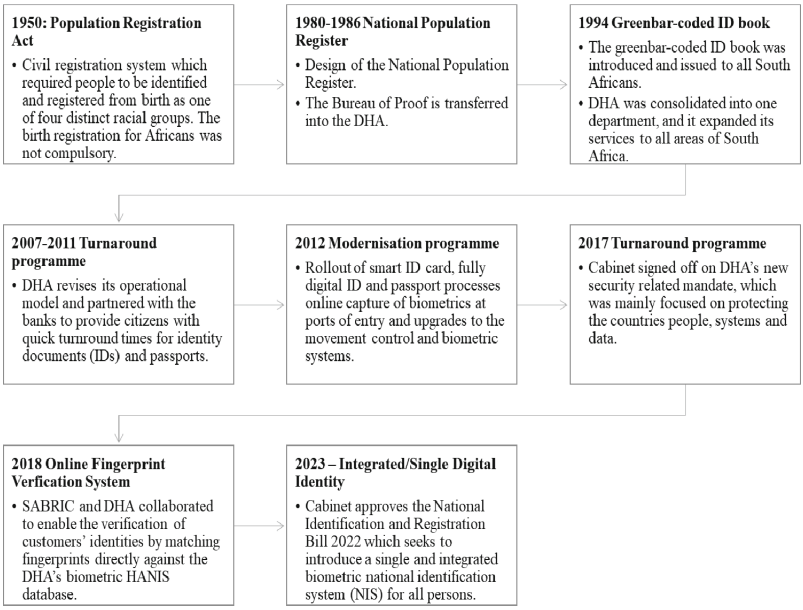

Fig. 1. South Africa's Digital Identity Roadmap.

South Africa is still a developing country and with that, it is still lagging in terms of digitisation and digital identity. However, the efforts made since the COVID-19 pandemic are essential towards the realisation of this in the country. This can be observed through the recent approval of the National Identification and Registration Bill of 2022 [10]. As it stands, the country could lean on the experiences of other countries that have successfully implemented this, but there are many considerations that must be acknowledged as this is pursued for a successful implementation in South Africa's context. According to Imprivata's digital identity maturity assessment categorisation, South Africa can be classified as *Phase 1: Initial* [11]. The five phases of digital identity maturity are depicted in Fig. 2 below.

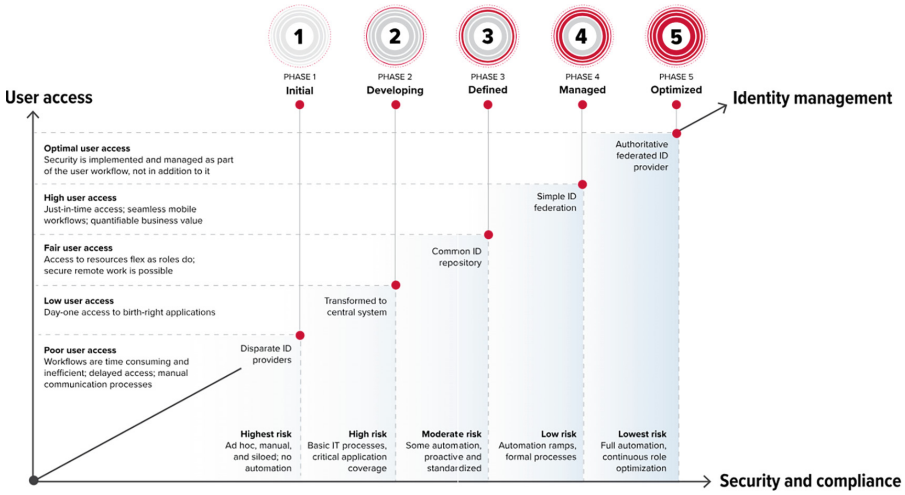

Fig. 2. Five phases of digital identity maturity.

3 Literature Review

3.1 International

This review focuses on digital identity frameworks proposed internationally by countries who are leading the digital identity space, specifically, [12] countries which are members of the Digital Identity Working Group, namely, Australia, Canada, Israel, New Zealand, Singapore, and European countries such as Finland, the Netherlands, and the United Kingdom (UK).

Australian government introduced the Trusted Digital Identity Framework (TDIF) which [13] as of August 2023, has thirteen policies which sets out the requirements that applicants must meet to achieve authorisation. The requirements presented in this framework includes Digital identity accreditation process, Functional Requirements which covers, Fraud control, Privacy, Protective Security, User Experience, Technical Testing, and Functional Assessments. Other requirements are Role Requirements which includes Common Role, Identity Service Provider, Credential Service Provider, Attribute Service Provider, and Identity Exchange. Additional requirements are Federation onboarding and Maintaining accreditation.

In Canada, the government introduced Pan-Canadian Trust Framework (PCTF) which was developed with a purpose of meeting the current and future Canadian digital identity ecosystem innovation needs by verifying trust of services and networks [14]. The PCTF includes ten components that should be considered when implementing a digital identity framework, which is; authentication, credentials, digital wallet, notice & consent, trust registries, verified person, verified organisation, assurance maturity model, glossary, and model. In addition, Canada's digital identity ecosystem is provided in [15] which is the integrated authentication and intermediary licensing model. This model includes four main elements of the ecosystem: An individual who seeks to provide identification to perform a digital transaction or interaction. The dependent section which

involves an organisation, individual, or system that requires access to an authority institution. An authority institution incorporates a certified, recognised, or trusted institution which provides warranty arrangements (related to credit or identity information) for dependent institutions.

In New Zealand, a Digital Identity Services Trust Framework was first introduced in 2021 and accepted in April 2023 [16]. It establishes rules to protect the privacy and security of people's information when shared within the trusted environment. This framework includes eight principles, such as the rights and needs of people and other entities involved in the digital identity system, governed by the Privacy Act. Inclusive of any entities and individuals without compromising security or privacy. Secure digital identity systems in the cyber and physical space. It is inclusive of Māori's perspectives, which caters for sustainability, interoperability, openness, and transparency.

In Singapore, [17] there is no specific legislation or framework for National Digital Identity presented. However, there are related legislations put in place to create Decentralised identifiers (DIDs). The key legislative acts include: The Public Sector (Governance) Act, which governs the management of data including personal data protection and data sharing. The Personal Data Protection Act, which provides a baseline standard of protection for personal data by the private sector in Singapore. Other legislations that support this act includes the Banking Act and Insurance Act. It governs the collection, use, disclosure, and care of personal data in Singapore—which is of vital importance to both privacy and trust in a digital identity ecosystem. The National Registration Act, which enables Singapore to retain a high-quality, high-coverage foundational ID system upon which Singpass is reliant. The Electronic Transactions Act, which is the key legal basis for Singpass by establishing trusted certification authority services in Singapore. It focuses on the facilitation of electronic transactions through the recognition of electronic signatures and records.

In Europe, digital identity regulations were introduced as described in [18], towards the development of the European Self-Sovereign Identity Framework (ESSIF) presented in [19] which incorporates digital identity ecosystem on the old regulations. These regulations provide an EU-wide framework for public electronic identities which ensures that any citizen or residents can have access to a secure European e-identity. These regulations include the following requirements to make-up the digital identity framework: objectives of the EU Digital Identity Wallet, roles of the actors of the DID ecosystem, wallet's functional and non-functional requirements, compliance with related standards, frameworks, and legislations, security, privacy, and trust.

Countries that are adopting the EU DID framework includes Finland, Netherlands, UK, and Israel. Finland, is still working towards self-sovereign identity frameworks, aligning with the EU Commission [12]. Finland is pursuing an ambitious schedule to introduce sovereign identity wallets like EU, to be available for people to provide various attributes, such as vaccination certificates, by 2023. Similarly, Netherlands has also been active in the development and participation in the electronic identification and trust services (eIDAS) regulation to create interoperable digital identity initiatives across the EU [12].

The UK's digital identity and attributes trust framework was developed to let individuals use and reuse their digital identities [20]. The trust digital identity framework

provides a set of rules that different organisations should follow. These includes legislation, standards, Good Practice Guides (GPGs) which are used to ensure products and services are inclusive, privacy and data protection, fraud management and security are highly considered. In addition, presented requirements are Privacy and data protection; Legal, technical and policy; Security; Both physical and cyber; Communications security (COMSEC); Fraud monitoring; Legal, policies and procedures for fraud management; Fraud reporting; Intelligence and fraud analysis; Sharing threat indicators ('shared signals').

In Israel, a system based on The International Organisation for Standardisation (ISO) standards was proposed and is anticipated to support future mutual recognition and interoperability [12]. Additionally, Israel is exploring compatibility with eIDAS standards and other international partners.

Other international research works includes work by researchers in [21] from the UK who proposed an open digital identity framework and architecture. This framework contributes to promoting the implementation of identity architectures while satisfying limitations that are considered important to the protection of human rights. The authors recommended a combination of strong technology such as Distributed Ledger Technologies (DLTs) and considerate policies shall be considered to promote and ensure the implementation, deployment, and the use of digital identity technology.

Another framework was introduced in Germany to improve security under the KYC theme [22]. Firstly, an eKYC architecture was proposed which involves three primary parties: the customer (holder), a bank (verifier), and an issuer (the same bank, another bank, or any third party trusted by the verifying bank, such as a government agency). The customer is the KYC subject and defines the centre of the architecture. The advantage of this framework is that customers manage their digital identity through user agents by creating and storing DIDs and cryptographic keys in their digital wallets. In addition, users can collect credentials, create backups, and manage permissions.

In [23], NIST provides a digital identity framework with four main components, namely; governance and administration (which includes compliance and risk mitigation of the DID system), identity management (this includes approved or qualified identity provider information and support and management of the DID system), authorisation, (may include roles and responsibilities for involved parties and individuals, policies and other regulation involved, data security and privacy, and identity assurance), last component is authentication and access (which is about access control, multifactor authentication, etc.

In [24] a DID framework was proposed for managing data in the department of health. Also, to provide Information Technology (IT) and security leaders with a toolkit to drive their Identity and access management (IAM) strategy. It addresses key governance principles for developing the DID ecosystem, related to required administration, identity management, authorisation, access, and authentication.

In 2018, the ITU from Switzerland reported a comprehensive report that contributes to the development of DID frameworks, the Digital Identity Roadmap Guide [8]. This guide presents guidelines covering the required design, development, and implementation of digital identity framework. In 2019, [25] authors presented a survey of digital identity architectures and their applications, focusing on the use of emerging standards

introduced by the World Wide Web Consortium (W3C) to ensure interoperability and portability throughout the SSI stack.

3.2 Africa

In the African context, research was conducted on aspects related to the state of digital identity in ten countries [26]. The project focus was on local foundational ID systems in countries such as Ghana, Kenya, Lesotho, Mozambique, Nigeria, Rwanda, South Africa, Tanzania, Uganda, and Zimbabwe. This research considered parameters set by an Evaluation Framework for Digital Identities (the 'Framework'), that was developed by the Centre for Internet and Society (CIS) with the purpose of assessing the alignment of digital identity systems for compliance with international rights and data protection norms. By using this Framework, the selected countries evaluated certain aspects of the existing governance and implementation mechanisms of digital identity in their respective and unique contexts. Moreover, the African Union Commission is currently working on a continental initiative to develop an interoperability framework for digital ID [27]. Amongst others, it draws efforts its mandate from the Digital Transformation Strategy (DTS) for Africa (2020–2030), which emphasises the importance of digitised legal identification mechanisms in the continent.

In 2019 [28] Nigerian organisation Secure Identity Alliance (SIA) initiated a programme for Open standards Identity APIs (OSIA) to develop a digital identity framework. This framework involves three main principles, sovereignty, technology neutrality, and privacy by design. The first principle (sovereignty) is about enabling ability of governments to choose what their ID solution will be, and which components are required in the digital identity ecosystem. The second principle promotes the value of deployed legacy technologies to be preserved, and freedom for governments to choose technology of their choice according to their needs. The third principle emphasize the importance of incorporating privacy by design on digital identity ecosystems while complying to legislations related to data privacy and security and enabling citizens to control access to their digital identity.

In South Africa, a case study and roadmap analysis were conducted by [29]. The findings showed that South Africa defined five important requirements for a DID system to meet: Identity management system and existing infrastructure, Frameworks and policies, Digital identity scheme administrator and committed stakeholders, Government endorsement and participation and the role of the private sector and Interoperability which involves the standardisation of the identity management infrastructure. Additionally, there are guiding principles to be considered when developing a DID system, categorised into three pillars, namely, inclusion, design, and governance. Inclusion encompasses principles to ensure universal coverage, and to remove barriers to access and usage of IT. Design involves values corresponding to establish a robust, unique, and secure programme, to create a platform that is interoperable, to use open standards and ensure technology neutrality, to plan for financial and operational sustainability and to protect user privacy and control. Lastly, governance involves principles to safeguard data privacy, security, and user rights through a comprehensive legal and regulatory framework, to establish clear institutional mandates and accountability, and to enforce legal and trust frameworks.

To our knowledge there has not been any research work conducted on comparing existing governance frameworks with the aim of learning from presented experiences to develop a country's governance framework. Thus, this paper presents a review of existing frameworks.

4 Digital Identity Frameworks

This section presents identified frameworks from the literature review conducted and presented in Sect. 3, and the results are presented in Table 1. To assess the identified frameworks, an assessment criterion has been defined.

4.1 Evaluation Criteria

According to [7], there are cross-cutting principles, which, collectively, can assist in the development of a progressive and holistic National Digital Identity Framework. These principles are:

- Vision and mission – set out goals to pursue, and how to achieve these goals.
- Comprehensiveness – all-encompassing understanding and analysis of the overall digital environment, considering the country's context, circumstances, and priorities.
- Social inclusiveness - should be developed such that its services cater for a community of users, with specific focus to vulnerable individuals and minority groups.
- Economic and social prosperity - should foster economic and social prosperity and maximise the contribution to sustainable development and social inclusiveness.
- Fundamental human rights - should respect and be consistent with fundamental human rights and values.
- Resilience - should enable an efficient risk management approach and ensure an appropriate level of resilience.
- Trust, privacy, and security - ensures adequate security measures are in place for maintaining information security, privacy and improve trust among users and stakeholders.
- Sustainability and cost optimisation - should be developed considering the economic sustainability of the system.
- Flexibility and scalability - must accommodate for efficient updates or modification when necessary.
- Interoperability - to ensure the ability of different systems to exchange information and queries.
- Speed of deployment - should follow a swift roll-out schedule.
- Identity as a platform - should foster the development of digital ID as a platform, so that users can plug it into any domain and use it.
- Uniqueness of IDs - ensures that people can get only one digital identity.
- Robustness and future-proofing technology – these include technologies and systems used for the creation of digital identities.
- Data quality - should serve as the base for other programmes of national importance; it is thus critical that steps are taken to ensure data quality at multiple levels.

These guidelines provide a great guide to when developing a framework focusing both on technical and non-technical aspect. Therefore, to assess these identified frameworks and to achieve a minimum viable digital identity framework, the following Assessment Criteria (AC) was followed:

- ***AC-1***: Does it support the SSI model? As there is a shift towards SSI it vital for the framework to support SSI implementations to align for future developments.
- ***AC-2:*** Does it support Interoperability? This is critical to ensure that the system can exchange information with different systems even on an international level.
- ***AC-3:*** Does it support DID framework/ecosystem?

4.2 Discussion

From the high-level assessment criterion defined in Sect. 4.1, we can compare all the frameworks and discover the most suitable framework/s to learn and derive from their experiences and expertise. It is worth noting that some frameworks have not specified other requirements due to either being architectures which therefore cannot specify for example model types. These are represented by "not specified" in Table 1. Out of the eleven identified frameworks, Table 1shows that, when compared against the assessment criterion; ESSIF, SSI4Web, PCTF, eKYC meets all the three requirements. These findings shows that Canada, Europe, and Germany are part of the countries that are leading Digital Identity, thus South Africa and other countries can learn from them.

The New Zealand Digital Identity Services Trust Framework is the secondary candidate for investigate and learn from especially because they have implemented and are about to roll out in 2024 [33]. Although for now it does not specify the use of DID ecosystem, it might support it in the future when the South African framework is drafted and implemented. The NIST digital identity framework [23] which focuses mainly on governance and administration, identity management, authorisation and authentication and access, will be beneficial in the development of the framework.

Other findings reveal that although other countries have adopted the use of digital identity, there is still more work required to address the support of SSI model to align for future developments, and to for the framework to support Interoperability to enable a secure information exchange with different systems even on an international level. These frameworks are presented in countries such as Nigeria (OSIA digital identity framework [28]), UK Government's Digital Identity and Attributes Trust Framework [30], The African Union (AU) Develops a Draft Interoperable Digital ID Framework for Africa [27], Digital identity framework [24, 31] originated in the United States, Australian Trusted Digital Identity Framework (TDIF) [13], and a Decentralized Digital Identity Architecture [21] from the United Kingdom.

It is worth noting that, Africa is also investing towards this topic whereby the AU has developed a draft Interoperable Digital ID Framework for Africa. Once it is finalised and agreed upon, it would make things easier especially the interoperability aspect of digital identities. Additionally, other frameworks are system or sector based like the TDIF which focuses on accreditation, thus limits the adoption of this framework. With the advancement towards SSI based solutions, it is vital to consider frameworks that cater for such, like ESSIF and SSI4Web (which also adds the aspect of password-less).

Table 1. Identified Digital Identity Frameworks.

Framework	Description	AC-1	AC-2	AC-3
OSIA digital identity framework [28]	An open standard set of interfaces (APIs) that enables, seamless connectivity between building blocks of the identity management ecosystem – independent of technology, solution architecture or vendor	Does not define the workflow between modules nor the architecture on any ID management solution	Yes	Not specified
UK Government's Digital Identity and Attributes Trust Framework [30]	Establishes a governance and oversight function and develops proposals to remove legislative and regulatory blockers to the use of secure digital identities and establish safeguards for citizens	No	Yes (plans to)	No
The African Union (AU) Develops a Draft Interoperable Digital ID Framework for Africa [27]	Proposes different models of the Identity Credentials such as Digi-tally signed credentials or digital wallets aimed at empowering citizens to have control over their personal data, while maintaining privacy and security	Not specified	Yes	Not specified

(*continued*)

Table 1. (*continued*)

Framework	Description	AC-1	AC-2	AC-3
Digital identity framework [24, 31]	Addresses key governance principles for developing the DID eco-system, related to required administration, identity management, authorization, access, and authentication	Not specified	Not specified	Yes
Trusted Digital Identity Framework (TDIF) [13]	Sets out requirements that applicants must meet to achieve accreditation. The accreditation framework and process ensure that all identity providers meet strict rules and standards for usability, accessibility, privacy protection, security, risk management, fraud control and more	Not specified	Yes	No
European Self-Sovereign Identity Framework (ESSIF) [19]	Implements a generic and interoperable SSI framework, defining the necessary specifications and building support services and capabilities that will allow citizens to control their digital identity	Yes	Yes	Yes

(*continued*)

Table 1. (*continued*)

Framework	Description	AC-1	AC-2	AC-3
Self-Sovereign Identity (SSI) Framework for the Web (SSI4Web) [32]	Integrates SSI for providing web services in a secure password-less manner with much more user control and greater flexibility	Yes	Yes	Yes
A Decentralized Digital Identity Architecture [21]	Defines a set of fundamental constraints that digital identity systems must satisfy to preserve and promote privacy as required for individual sovereignty. Authors proposed a decentralized, standards-based approach, using a combination of DLT and regulations, to facilitate many-to-many relationships among providers of key services	Not specified	Not specified	No
Pan-Canadian Trust Framework (PCTF) [14]	Designed to meet current and future Canadian digital identity ecosystem innovation needs by verifying trust of services and networks	Yes	Yes	Yes

(*continued*)

Table 1. (*continued*)

Framework	Description	AC-1	AC-2	AC-3
Germany framework for digital identity Know Your Customer (KYC) [22]	Presents an Electronic Know Your Customer (eKYC) architecture involving three primary parties: holder, verifier, and an issuer	Yes	Yes	Yes
New Zealand Digital Identity Services Trust Framework [16]	First introduced to establish rules to protect the privacy and security of people's information when shared amongst organisations in the trusted environment	Yes	Yes	No

5 Conclusion

In this digital age, the use of digital identities will increase exponentially and with that the need to have governance frameworks in place to control how these identities are issued, maintained, and authenticated. This provides opportunities for researchers and decision-makers to study the trend of governance frameworks. This is crucial for South Africa as currently; centralised models are utilised for identities. The country is making formidable strides in closing existing gaps of citizens lacking identities and moving towards social inclusion, as well as moving towards digitisation. However, the country is still at the initial stages of digital identities. The goal of this study was to understand what other countries have done towards developing governance frameworks for digital identities, specifically developed countries as they are already ahead with digitisation. In understanding these frameworks, we can draw conclusions and work towards, defining a framework or combination of frameworks suitable for South Africa.

In this study, we investigated existing literature on digital identity frameworks worldwide, eleven frameworks were identified and compared against a defined assessment criterion. While this list is not exhaustive, it paints a picture of the existing gap especially in Africa and paves a way for South Africa to develop its own framework, learning from these existing frameworks. We hope that our review will help guide the field in providing clarity and advance the field. Digital identity models have moved from centralised to decentralised and due to their new/evolving nature, it is vital that we keep abreast of any improvements. With the high-level assessment criteria presented in this study, and there is a possibility for change in future as the field gains traction. Hence, it is vital to remain updated with these improvements.

References

1. Clark, J., Diaphasia, A., Casher, C.: 850 million people globally don't have ID-why this matters and what we can do about it. World Bank Blogs   (2023);. https://blogs.worldbank.org/digital-development/850-million-people-globally-dont-have-id-why-matters-and-what-we-can-do-about. Accessed 16 Aug 2023
2. 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 (2019). https://www.worldbank.org/en/news/immersive-story/2019/08/14/inclusive-and-trusted-digital-id-can-unlock-opportunities-for-the-worlds-most-vulnerable. Accessed 16 Aug 2023
3. Preukschat, A., Reed, D.: Self-sovereign identity. Manning Publications (2021)
4. Ndung'u, N.S., Signé, L.: Capturing the fourth industrial revolution: a regional and national agenda. (2020)
5. Digital Transformation Agency. Digital Identity. Digital Transformation Agency (2023, July 3). https://www.dta.gov.au/our-projects/digital-identity. Accessed 16 Aug 2023
6. Kiourtis, A., et al.: Identity management standards: a literature review. Comput. Inform. **3**(1), 35–46 (2023)
7. I. Fernmelde-Union. Digital identity roadmap guide (2018)
8. International Telecommunication Union, Digital Identity Roadmap Guide (2018). https://www.itu.int/pub/D-STR-DIGITAL.01-2018. Accessed 20 Jul 2023
9. Thales. Digital Identity Trends – 5 forces that are shaping 2023. Thales Group (2021). https://www.thalesgroup.com/en/markets/digital-identity-and-security/government/identity/digital-identity-services/trends. Accessed 16 Aug 2023
10. Department of Home Affairs. National identification and registration bill: Draft. South African Government. https://www.gov.za/documents/national-identification-and-registration-bill-draft-18-apr-2023-0000 Pierucci, Federico, and Valeria Cesaroni. "Data Subjectivation-Self-sovereign Identity and Digital Self-Determination." Digital Society 2.2 (2023). Accessed 16 Aug 2023
11. Imprivata. Digital identity maturity assessment. https://www.imprivata.com/assess. Accessed 20 Aug 2023
12. DGX (Digital Gov Exchange) Digital Identity Working Group. "Digital identity in response to covid-19." Digital Transformation Agency (2022)
13. Australian Government. Trusted Digital Identity Framework (TDIF) | Digital Identity. https://www.digitalidentity.gov.au/tdif. Accessed 20 Jul 2023
14. The Digital Identification and Authentication Council of Canada (DIACC). Trust Framework. Digital ID Authentication Council of Canada, April 2023. https://diacc.ca/trust-framework/.Accessed 17 August 2023
15. Rasouli, H., Valmohammadi, C., Azad, N., Abbaspour Esfeden, G.: Proposing a digital identity management framework: a mixed-method approach. Concurrency Comput. Pract. Experience **33**(17), 62–71 (2021)
16. Hon Dr D. Clark.: Digital Identity Services Trust Framework bill - New Zealand legislation (2023). Available at: https://www.legislation.govt.nz/bill/government/2021/0078/latest/LMS459583.html?src=qs Accessed 17 August 2023
17. World Bank. National Digital Identity and Government Data Sharing in Singapore: A Case Study of Singpass and APEX. World Bank (2022)
18. European Commission. The Digital Services Act: Ensuring a safe and accountable online environment. European Commission (2022, October). https://commission.europa.eu/strategy-and-policy/priorities-2019-2024/europe-fit-digital-age/digital-services-act-ensuring-safe-and-accountable-online-environment_en. Accessed: 20 July 2023

19. Du Seuil, Daniel. European Self Sovereign identity framework (2019)
20. Department for Science, Innovation and Technology, Department for Digital, Culture, Media & Sport, and Warman M. "UK digital identity and attributes trust framework alpha v2 (0.2)" (2023). https://www.gov.uk/government/publications/the-uk-digital-identity-and-attributes-trust-framework/the-uk-digital-identity-and-attributes-trust-framework. Accessed 16 Aug 2023
21. Zwitter, A., Cooper, N., Zambrano, Goodell, R.G., Aste, T.: A decentralized digital identity architecture," Frontiers in Blockcha*in*| www.frontiersin.org **2**(17), 1–19 (2019)
22. Schlatt, V., Sedlmeir, J., Feulner, S., Urbach, N.: Designing a framework for digital KYC processes built on blockchain-based self-sovereign identity. Inf. Manag. **59**(7), 103553 (2022)
23. National Institute of Standards and Technology. NIST Special Publication 800–63BNIST Special Publication 800–63B Digital Identity Guidelines Authentication and Lifecycle Management (2022). NIST Special Publication 800–63B. Retrieved July 20, 2023, from https://pages.nist.gov/800-63-3/sp800-63b.html, https://identitymanagementinstitute.org/nist-digital-identity-summary-and-update/
24. Imprivata, Digital identity framework | https://www.imprivata.com/digital-identity-framework. Accessed: 20 July 2023
25. Avellaneda, O., et al.: Decentralized identity: Where did it come from and where is it going? IEEE Commun. Stan. Mag. **3**(4), 10–13 (2019). https://doi.org/10.1109/mcomstd.2019.9031542
26. Research ICT Africa, & Spuy, A. van der. Ria releases 10 country reports on Digital ID framework. Research ICT Africa (2021). https://researchictafrica.net/2021/11/09/ria-releases-10-country-reports-on-digital-id-framework/. Accessed 16 Aug 2023
27. The Lawyers Hub, The AU Develops a Draft Interoperable Digital Id Framework for Africa, https://lawyershub.org/blog/The_Au_Develops_A_Draft_Interoperable_Digital_Id_Framework_For_Africa_30. Accessed 20 July 2023
28. Nigeria National Identity Management Commission (NIMC). Unlocking the ID Ecosystem with OSIA: A universal interoperability framework for innovation, competition, and sustainability (2022). OSIA. Retrieved July 20, 2023, from https://secureidentityalliance.org/osia
29. Razzano, G.: Digital Identity in South Africa: Case study conducted as part of a ten-country exploration of socio-digital ID systems in parts of Africa. Research ICT Africa (2021). https://researchictafrica.net/publication/digital-identity-in-south-africa-case-study-conducted-as-part-of-a-ten-country-exploration-of-socio-digital-id-systems-in-parts-of-africa/. Accessed 16 Aug 2023
30. UK digital identity and attributes trust framework alpha v1 (0.1) - GOV.UK, https://www.gov.uk/government/publications/the-uk-digital-identity-and-attributes-trust-framework/the-uk-digital-identity-and-attributes-trust-framework. Accessed 20 July 2023
31. Cairns, K., Wright, W.: The Imprivata digital identity framework: A guide for IT leaders in healthcare. Imprivata (2022)
32. Ferdous, M.S., Ionita, A., Prinz, W.: SSI4Web: A Self-sovereign identity (SSI) framework for the Web. In: International Congress on Blockchain and Applications. Cham: Springer International Publishing (2022)
33. Burt, C.: New Zealand digital identity trust framework law passes. Biometrics News. https://www.biometricupdate.com/202303/new-zealand-digital-identity-trust-framework-law-passes. Mar 30, 2023