African Union

An Integrated, Prosperous and Peaceful Africa

AU INTEROPERABILITY FRAMEWORK FOR DIGITAL ID

FEBRUARY 2022

CONTENTS

EXECUTIVE SUMMARY

Millions of people in Africa lack legal identification (ID), and many more have IDs that are not fit for purpose in the digital age. As a result, they are facing challenges to access services and opportunities being created through digitalisation. Therefore, interoperable, trusted and inclusive digital foundational IDs, which provide people with the ability to verify their legal identity offline and online, can help to address those challenges and have significant potential to accelerate the digitalisation of African economies and societies by supporting entrepreneurship and contributing to the successful implementation of the African Continental Free Trade Area (AfCFTA). It is for these reasons that most African countries are currently modernising their ID ecosystems, although they are at different stages of doing so.

The AU Interoperability Framework for Digital ID (the Framework) sets out a vision that will **enable all African citizens to easily and securely access the public and private services they need, when they need them, and independently of their location**. To this end, the Framework defines common requirements, minimum standards, governance mechanisms, and alignment among legal frameworks. Its objectives include the need to:

1. allow African citizens to verify their legal identity offline and online to access public and private sector services in AU Member States. This can contribute to continental unity and integration for sustained growth, trade, exchanges of goods, services, free movement of people and capital by establishing a united Africa and fast-tracking economic integration through AfCFTA, as stated in aspiration 2 of the Agenda 2063;

2. empower African citizens with control over their personal data, including the ability to selectively disclose only attributes that are required for a particular transaction. Personal information that is disclosed should be minimal, proportionate, only contain the information relevant to that specific transaction, in line with international best practices;[1] and

3. strengthen trust and interoperability among foundational identification systems of AU Member States.

The Framework provides for a common standard at the continental level to represent, digitally, the proofs of identity issued by trusted sources from AU Member States and to ensure interoperability throughout the continent. Individuals who hold an ID from a national system will be able to obtain an interoperable, digital credential for legal identity (IDC-ID) that will take the form of a verifiable claim[2]. Standards will be established for the interoperability framework that will define key elements of the IDC-ID. These standards will operate to demonstrate trust in the IDC-ID as created under the governance of a Trust Framework that defines the conditions under which trusted sources from the AU Member States will issue such credentials.

1 See, The EU General Data Protection Regulation (GDPR), 2016: https://gdpr.eu.

2 'Claims' are a collection of attributes about a data subject: e.g., family name or date of birth. A 'verifiable claim' is a tamper-evident version of this information which can be cryptographically verified in order to check its authenticity.

AU Member States have the freedom to select how they want to issue this digital credential. It may be stored in a purely digital format on a smartphone application, a cloud-based server, a smartcard, or a link to the digital representation may be established using a one- or two-dimensional barcode on a paper document (printed on paper, plastic card). Member States can also decide to reuse this standard to represent identity data at the national level, as part of a continental or Regional Economic Community (RECs) level, or even issued separately to complement existing digital ID systems.

The Framework will be based on the development of interoperable, inclusive, and trusted foundational ID systems as these provide the backbone of authoritative sources of data on people's legal identity and thus enable the IDC-ID to achieve higher levels of assurance. AU Member States are therefore encouraged to strengthen their foundational ID systems, taking into consideration supportive mechanisms like the *Principles on Identification for Sustainable Development*.[3] This Framework will also take into account and builds upon parallel continental efforts to create an enabling environment aiming at protecting personal data, maintaining cyber security, and safeguarding people's rights, with the adoption of the *African Union Convention on Cyber Security* and *Personal Data Protection* (Malabo Convention)[4] and ongoing work to develop a continental data policy framework.

The issuance of the IDC-ID can be completed with an infrastructure enabling more advanced use cases such as remote authentication. This Framework highlights several technical options available to AU Member States to implement this layer. Examples include a federation of identity providers providing authentication mechanisms to the holders of the IDC-ID, the development of digital ID wallet solutions, or any other models enabling interoperability. AU Member States will also be able to seek further agreement on how to establish this authentication layer infrastructure and partner with RECs and other continental initiatives that are already investigating the introduction of interoperable foundational digital ID solutions to access services remotely.

The success of the proposed Framework is based on the assumption that it will be adopted and endorsed by AU members States. To do so, certain risks must be mitigated and addressed, and challenges must be overcome, including the risk of exclusion, weak security mechanisms, the risk of eroding personal privacy, a lack of demand (often due to uncertainties about the benefit of foundational digital ID systems), a lack of technical and financial capacities, a dearth of data centres (important for storing sensitive data) across Africa, the presence of non-inter-operable ID systems, and outdated legal and regulatory frameworks. (These challenges are addressed in more depth in section 5 below.)

3 The Ten Principles on Identification for Sustainable Development have been endorsed by 30 international and regional organisations, including African institutions such as UNECA, AfDB and Smart Africa, as well as adopted by a number of African countries. See: https://id4d.worldbank.org/principles.

4 African Union (2014), Convention on Cyber Security and Personal Data Protection, see: https://au.int/en/treaties/african-union-convention-cyber-security-and-personal-data-protection.

The document comprises of the following sections:

1. A **background** section on the work of the AU that has led to the creation of this document, an overview of the state of ID systems in Africa, and a series of initiatives promoting the interoperability of digital IDs on the continent.
2. An **introduction** to the vision, objectives, scope and potential use cases for the proposed Framework.
3. An overview of the **key elements constituting the Framework**, notably guiding principles for its design and implementation, the model selected, the key components of the framework that will have to be further defined (e.g., rules of participations, interoperability, and technical requirements), as well as three potential architectural options to set up an interoperability authentication layer.
4. **A high-level roadmap** elaborates on the proposed phased approach for the definition and implementation of the Framework, as well as concrete actions that might be taken by Member States and the AU.
5. **High level assumptions, challenges**, risks to be addressed, and recommended mitigation mechanisms.

The Framework does not call for the creation of a unified continental digital ID system but calls for establishing an interoperability framework for existing foundational digital ID systems among AU Member States that considers the digital sovereignty of AU Member States, the differences in the digital infrastructure rollout, the availability of associated policies and regulations, the different types of ID systems, and the vulnerability of populations during and after the implementation of the interoperable digital ID systems.

ACRONYMS AND ABBREVIATIONS

AfCFTA	African Continental Free Trade Area
AML/CFT	Anti-Money Laundering/Combating Financing of Terrorism
API	Application Programming Interface
AU	African Union
AUC	African Union Commission
CIRTs	Computer Incident Response Teams
CRVS	Civil Registration and Vital Statistics
DPA	Data Protection Authority
DPIA	Data Protection Impact Assessment
EAC	East African Community
ECOWAS	Economic Community of West African States
GIZ	Gesellschaft für Internationale Zusammenarbeit
GSMA	GSM Association
HSMs	Hardware Security Modules
ICT	Information and Communication Technology
IDC-ID	Interoperable Digital Credential for Identity
ITU	International Telecommunications Union
KYC	Know-Your-Customer
LOA	Level of Assurance
PATF	Pan African Trust Framework
REC	Regional Economic Community
RP	Relying Party
SATA	Smart Africa Trust Alliance
The Framework	AU Interoperability Framework for Digital ID
UNECA	United Nations Economic Commission for Africa
WURI	West Africa Unique Identification for Regional Integration and Inclusion

See Annex I for working definitions.

1. BACKGROUND

1.1. CONTEXT

Being able to prove one's identity is essential for their ability to access services and exercise certain rights. Traditionally, proving identity could be done on the basis of familiarity, appearance and vouching by others, which worked in smaller, informal communities. As societies and economies became larger, more formalised and more integrated, physical credentials such as ID cards and passports were introduced to establish trust. However, as countries shift to digital societies and economies, such physical credentials are not very useful for proving identity over the Internet and carrying out other digital transactions such as digital payments and sharing personal data. A prerequisite for trust online therefore are digital identities, represented by digital IDs that use modern technologies and approaches to enable people to securely prove and verify their identity online.

IDs and, in particular, digital IDs can provide a wide range of benefits for countries. Some examples include good governance, financial inclusion, gender equality and the empowerment of women, enhanced social protection, healthcare and education outcomes. For individuals, digital IDs provide a tool to assert their rights and eligibility for services and transactions. For governments and businesses, digital IDs provide a platform to streamline, expand and innovate their operations' service delivery through the use of digitalisation and automation, especially when envisioned as a 'digital stack' with trusted data sharing and digital payment platforms.[5] Considering that the Internet has no borders, digital IDs that are issued in one country and recognised in others can also be a powerful driver of social and economic integration, whether at the bilateral, regional or global levels.

Digital IDs achieve the greatest security and impact when they are based on the legal identity of individuals. Legal identity is typically managed by a country's foundational ID ecosystem, including civil registration, national ID, and other similar systems. However, millions of people in Africa are still lacking foundational identification such as a national IDs or birth certificates.[6] It is in this context that, in July 2016, the AU Assembly declared 2017 to 2026 as the decade for repositioning CRVS in Africa as a priority on the continental, regional and national development agenda. It also urged governments to respond with appropriate action.

*Agenda 2063: The Africa We Wan*t, which is the strategic framework for the socio-economic development and transformation of the continent within a period of 50 years, has called for legal identity for all. The *Digital Transformation Strategy for Africa* (DTS), endorsed at the 36th Ordinary Session of the African Union Executive Council in February 2020 in Addis Ababa, Ethiopia (EX.CL/Dec. 1074 (XXXVI), also underscored the importance of digital ID as a building block for the establishment of a Digital Single Market (a mission that is also shared by the Smart Africa Alliance) in line with the African Continental Free Trade Area (AfCFTA).

5 COVID-19 has highlighted the importance of digital stacks as the countries with these fully or partially in place before the pandemic began were better able to quickly and effectively deliver social assistance and were more resilient when in-person services had to be moved online.

6 World Bank (n.d.), Global ID4D Dataset, see: https://id4d.worldbank.org/global-dataset.

The DTS also recognised that the development of the digital economy and society relies on important enablers, notably a strong enabling environment with regard to cyber security and data protection. The 2014 *Convention on Cyber Security and Personal Data Protection* (the Malabo Convention)[7] provides a legal, policy and regulatory framework that enables the establishment of a safe digital environment for digital transaction, e-commerce, and the transfer of personal data. Unfortunately, this legal framework has not yet been signed and ratified by the required number of AU Member States for it to enter into force, effectively limiting its efficacy.[8] Once in effect, such a legal framework will not only contribute to the promotion of the trust in the Framework and inclusion, but will also mitigate risks linked to unauthorised surveillance and discrimination, particularly for vulnerable or marginalised groups, as well as ensure accountability for implementing authorities.

1.2 THE STATE OF ID SYSTEMS IN AFRICA

Trusted and inclusive ID systems are an enabler for many development outcomes such as eliminating poverty, promoting good governance, enabling safe and orderly migration, facilitating social protection, and promoting gender equality. They are also an important driver of digital transformation. Given the fundamental need for secure and accurate online identification and authentication, digital ID and other trust services — such as digital signatures — represent the next frontier for countries of the continent. When enabled by digital infrastructure that brings people and organisations online, digital ID and trust services can be leveraged by government and commercial platforms to facilitate a variety of digital transactions, including digital payments. At a country level, digital ID could act as a unique identifier for citizen-centric systems, making it viable to integrate systems. Together, digital ID and payments platforms provide the means to move towards cashless societies, creating productivity gains, reducing corruption and fraud, and improving user convenience and benefit.

A wide range of ID system types exist across the continent, with different levels of development linkages with service delivery. Many countries are in intermediate levels of development, with coverage gaps among vulnerable populations and nascent digital capabilities, while others have newly emerging or non-existent foundational ID systems. Overall, however, the number of countries implementing national ID systems has increased exponentially during the past two decades, driven by the desire to improve the efficiency of government payments and transfers; to enhance the integrity of elections; to improve financial sector services (via know-your-customer (KYC) and SIM registration); to enhance public security; and to promote safe and orderly migration. There is also continued momentum to reform and modernise system design and implementation approaches in line with the expanding evidence on good practices and lessons learnt from successful ID programmes elsewhere.[9]

An example is Rwanda, which has conducted a campaign to digitise its economy and empower its middle class by conducting actions like the move to a cashless economy, which the government aims to achieve through ubiquitous mobile phone penetration and high-speed Internet access. Rwanda joined the Better Than Cash Alliance, a global partnership committed to moving from cash to digital payments. The country is already realising the increased

7 AU (2014), Convention on Cyber Security and Personal Data Protection, see: https://au.int/en/treaties/african-union-convention-cyber-security-and-personal-data-protection

8 As of July 2021, 14 Member States out of 55 have signed the Malabo Convention (ibid), among which 10 Member States have ratified it. To enter into force, ratification by at least 15 Member States is required.

9 A 2018 survey of African government officials revealed that 60 percent of African countries were planning to launch an ID system or modernise the existing one by the end of 2020.

efficiency and revenue generated by eliminating collection costs and other expenses. Rwanda is also sharing best practices with others interested in pursuing a similar path.[10]

The digital capabilities of ID systems have increased greatly, although digital identification in the context of online transactions is still in its infancy. Over the past decade, many countries have embarked on efforts to modernise their identification systems, with the goal of creating a digital platform and issuing credentials that underpin a variety of uses and services. These reforms frequently involve a transition from paper-based toward digital systems using electronic data capture and data management. They also commonly involve introducing digital ID verification and authentication mechanisms – for now, mostly in the context of in-person transactions.

The majority (85%) of African countries have national ID systems underpinned by an electronic database, although many still rely on paper-based civil register and processes, and many systems offer limited utility for service delivery. Biometric data is collected by more than 70 percent of African countries at the time of registration to ensure the uniqueness of identities. Although some countries – such as Kenya, Lesotho, Nigeria, Rwanda, South Africa – offer digital ID verification services (to government ministries, banks, etc.) to validate identity information or credentials against a central database, authentication for most transactions continues to rely on the manual inspection of physical ID cards. Digital ID solutions that enable secure authentication for online services and transactions are still in their infancy on the continent, with such services only available in a handful of countries (e.g., in South Africa by banks, or in Cabo Verde and Seychelles for eGovernment services).

Despite many improvements and the launch of new systems in recent years, African countries and their residents face several challenges when it comes to identification. Some of the key areas that required strengthening include the accessibility of ID systems, their ability to effectively support service delivery, and the implementation of safeguards that promote trust and data privacy.

Ensuring universal accessibility of ID systems is an ongoing challenge. An estimated 1 billion people around the world lack basic identity documents – and approximately half of that population reside in Africa.[11] Africa is also home to 8 of the 10 countries with the largest ID gender gaps globally and ID coverage among adults in Sub-Saharan Africa is close to 10 percentage points lower among women than men.[12] Challenges in identification start from birth: 100 million children under the age of five in Africa have not had their birth registered.[13] The reasons for these coverage gaps are manifold and include high direct and indirect costs of enrolment, including the cost of travel to often-distant registration sites; complex documentary and administrative requirements for registration; and limited demand where ID systems offer limited value in terms of facilitating access to services.[14]

The use of modern technologies has also increased complexity and presented new risks. For example, not all digital ID solutions are well-adapted to local needs and contexts where Internet connectivity, access to electricity, or digital literacy among civil servants or the general

10 ITU/DIAL (2019) SDG Digital Investment Framework, see: https://www.itu.int/pub/D-STR-DIGITAL.02-2019
11 ID4D (2018) ID4D Global Dataset, see: https://id4d.worldbank.org/global-dataset
12 ID4D (2017) Findex Survey 2017, see: https://documents1.worldbank.org/curated/en/727021583506631652/pdf/Global-ID-Coverage-Barriers-and-Use-by-the-Numbers-An-In-Depth-Look-at-the-2017-ID4D-Findex-Survey.pdf
13 UNICEF (2019) Birth registration for every child by 2030, see: https://www.unicef.org/media/62981/file/Birth-registration-for-every-child-by-2030.pdf.
14 World Bank (2017) The state of Identification Systems in Africa, see: https://documents1.worldbank.org/curated/en/156111493234231522/pdf/114628-WP-68p-TheStateofIdentificationSystemsinAfricaASynthesisofIDDAssessments-PUBLIC.pdf.

population may be limited. Vendor lock-in is also a common concern, and is often associated with unsustainably high operating costs, limited interoperability of the ID system, and low levels of government and individual oversight and control over identity data. In addition, with the increased adoption of digital technologies in identification and authentication as well as the shift toward digital credentials, people with limited (digital) literacy skills and access to connected devices risk being left further behind.

As systems and data processing becomes digitised, the need to implement effective safeguards to protect data and individuals' privacy has increased. Inadequate safeguards for data protection, privacy, and user rights – whether legal, institutional, or technological – can leave ID systems vulnerable to breaches and people's data unprotected. Many countries still have a long way to go in building secure and trusted ID systems: only 28 countries (50%) in Africa have reportedly adopted data protection and privacy legislation and 39 (70%) African countries have cybercrime legislation in place.[15] Even where and when such frameworks do exist, translating legal provisions into effective institutional, operational, and technical controls can be challenging. As of today, only a few countries store and manage their data according to international best practices to protect against theft or unintentional data loss, for example.[16]

Digital ID systems are faced with similar challenges as digital ecosystems development. These challenges include funding issues, because funding cycles (mainly donor-based ones that are project-based and time-bound), tend to be disconnected from tech development cycles. There is also often a lack of funding available for scaling up ICTs, as funds tend to be available only for the stages of the technology development life cycle, with limited funding available for scaling up at national level. Besides funding and financing, planning tends to happen in silos and decision-making across stakeholder groups lead to limited opportunities for coordination among stakeholder groups. Such siloed approaches tend to limit the reuse of digital solutions and undermine their potential applicability across programmes and sectors. Deficiencies in digital literacy, including lack of capacity in ICT leadership, and in the selection, design, implementation, scaling up, and maintenance of ICT solutions, are often an issue among governments and development practitioners.[17]

1.3 OTHER INITIATIVES

A number of existing initiatives complementary to the Framework promote the mutual recognition and interoperability of digital IDs in Africa. These include, but are not limited to:

1.3.1. DIGITAL TRANSFORMATION STRATEGY FOR AFRICA (2020-2030)

Digital ID is recognised as one of five cross-cutting themes of the Strategy, which also makes ten policy recommendations and proposes actions across two themes of ensuring inclusion, security, privacy and data ownership, and supporting interoperability and neutrality. While

15 UNCTAD (n.d.) Data Protection and Privacy Legislation Worldwide (database), see: https://unctad.org/en/Pages/DTL/STI_and_ICTs/ICT4D-Legislation/eCom-Data-Protection-Laws.aspx.
16 World Bank (2017) The state of Identification Systems in Africa, see: https://documents1.worldbank.org/curated/en/156111493234231522/pdf/114628-WP-68p-TheStateofIdentificationSystemsinAfricaASynthesisofIDDAssessments-PUBLIC.pdf.
17 ITU/DIAL (2019) SDG Digital Investment Framework, see: https://www.itu.int/pub/D-STR-DIGITAL.02-2019.

these recommendations mainly cover the development of national digital ID systems, one recommendation does call for the establishment of a "continental interoperable and open digital ID, allowing validation and authentication of individuals," while another recommendation requests the AUC, United Nations Economic Commission for Africa (UNECA), and other partners to "work together on continental and regional standards, including on authentication protocols, minimum data fields, deduplication protocols, biometric formats as well as other formats, model regulations, and other standards".

1.3.2. UNECA INITIATIVE ON DIGITAL ID

UNECA has launched an initiative on digital ID, trade and digital economy (DITE), acting as a Centre of Excellence, which aims at harmonising related standards, adopting regulations to safeguard security, upping investments, and developing the capacity and skills of key actors.[18] The ECA Digital Centre of Excellence supports the work aiming at establishing a harmonised Framework, defining and shaping policies and standards for digital ID, providing capacity development for Member States, RECs, and the AU. The ECA has also produced a white paper on a framework for digital interoperability through the establishment of a Pan African Trust Framework (PATF).

1.3.3. SMART AFRICA TRUST ALLIANCE (SATA)

Smart Africa is an initiative of African Heads of State to accelerate the socio-economic development in Africa by leveraging ICT. In 2020, Benin championed a Smart Africa flagship project to develop the Digital ID Blueprint, supported by a working group that included Rwanda, Tunisia, the AU, the International Telecommunications Union (ITU), the World Bank, Omidyar Network, UNECA, the GSM Association (GSMA), the World Economic Forum, the Gesellschaft für Internationale Zusammenarbeit (GIZ), and several private companies. It was adopted by the Smart Africa Board, including its 32 Member States, the AU, and the ITU. The Blueprint[19] proposes SATA as a platform to facilitate the trusted recognition of digital IDs between a range of actors through federated certification mechanisms. Pilot projects of SATA are anticipated to take place in Benin, Rwanda, Tunisia, and other Smart Africa Member States. SATA will serve as an agile and adaptable solution to enable interoperability between various public and private identity schemes on the continent. More details will be available on sata.smartafrica.org.

1.3.4. WEST AFRICA UNIQUE IDENTIFICATION FOR REGIONAL INTEGRATION AND INCLUSION (WURI) PROGRAM

WURI [20] is a regional program that leverages financing from the World Bank to increase access to services in participating Member States from the Economic Community of West African States (ECOWAS). It does so by building foundational ID systems that are accessible to all persons in the territory of the country—without consideration for nationality or legal status—and are designed with cross-border interoperability in mind to unlock access to social, health, financial and other services across borders. Côte d'Ivoire, Guinea and the ECOWAS Commission joined in phase one in 2018, and Benin, Burkina Faso, Niger and Togo joined in phase two

18 UNECA (n.d.), DITE for Africa, see: https://www.uneca.org/dite-africahttps://www.uneca.org/dite-africa.
19 Smart Africa (2020, October) Blueprint | Smart Africa Alliance – Digital Identity, see: https://smartafrica.org/knowledge/digital-id/.
20 World Bank (n.d.) West Africa Unique Identification for Regional Integration and Inclusion (WURI) Program, see: https://projects.worldbank.org/en/projects-operations/project-detail/P161329.

in 2020. Key principles of WURI include universally accessible and inclusive registration, data minimisation, and basic credentials that are provided at no cost to the population.

1.3.5. EAC COMMON MARKET PROTOCOL

Through Article 8 of the Protocol, the six East African Community (EAC) Partner States have committed to work progressively towards "…a common standard system of issuing national identification documents to their nationals."[21] This is strongly linked to achieving other objectives of the Protocol, including the free movement of goods (Article 6), persons (Article 7), labour/workers (Article 10), services (Article 16), and capital (Article 24), as well as the rights of establishment and residence (Articles 13 and 14, respectively). However, the national ID systems are at varying stages of development. Nonetheless, in the spirit of variable geometry and as an initiative of the National Corridor Integration Projects (NCIP), Kenya, Rwanda and Uganda began recognising each other's national ID cards as valid travel documents in 2014. Within the framework of NCIP there have been discussions to build on this for additional use cases such as e-services, but these have not yet materialised. In 2018, the World Bank and EAC secretariat conducted a study on options for mutual recognition of national IDs (NIDs) in the EAC, and proposed four milestones.

1.4. DIGITAL AND DATA SOVEREIGNTY

With 55 sovereign nations, Africa has 55 legal jurisdictions to be considered when developing policy instruments. Digital sovereignty describes a spectrum of different technical and regulatory concepts, ranging from the physical location of servers and the construction of undersea cables, to laws and practices pertaining to cybersecurity, data protection and the taxation of data markets, that enable States to make their own decisions on technological choices and their regulation.

In order to guarantee digital and data sovereignty,[22] AU Member States are encouraged to:

Establish secure storage systems for personal data (including sensitive data) by designing and setting up national data centres which must provide for data control by the State and include at least storage and processing space devoted exclusively for personal and sensitive data. It will be necessary to put in place required safeguards (technical, in particular) to ensure that data which are used in cross-border information exchanges do not in any way include personal or sensitive data whose processing or storage would pose risks to the rights of individuals or the sovereignty of AU member States.

21 EAC (2020), see: https://www.eac.int/images/doc_image_png_NnlwzXikEvuHdytNzkKNVDMScreen%20Shot%202017-06-20%20at%20153445.png.

22 'Data sovereignty' as used in this Framework has the following meaning: personal data (including sensitive data) related to digital identification systems in an AU Member State must be collected, stored and processed (i) in facilities owned or controlled by and (ii) under the applicable law of the AU Member State.

Build capacity and infrastructure for the development of African talents and skill sets to meet the new challenges and strengthen the digital sovereignty. Member States are expected to take the lead in advancing the skills (including cyber resilience skills) of all citizens and residents, and should empower people to have control over their personal data.

Establish partnership based on mutual respect, win-win situation without compromising sovereignty and national ownership and avoids foreign interferences which may negatively affect the national security, economic interests and digital developments of AU Member States.

The Framework will be guided by the sovereign rules represented by each AU Member State's registration and identity issuing authority or authorities, and the proposed governance structure including the establishment of a continental coordinating institution to be endorsed by AU Member States. Furthermore, accountability mechanisms including the handling of liabilities in case of misconduct will be defined and endorsed by AU Member States. Developing continental trust among sovereign states with divergent digital identification schemes is a complex but achievable task requiring multi-stakeholder collaboration. To achieve interoperability for the exchange of legal identity information in respective African countries, the commonalities between existing national rules and standards must be recognized, based on a minimum set of criteria which will allow both local sovereignty and sufficient trust in each other's approach.

For this purpose, AU Member States need to strengthen and enhance their legal frameworks and enforcement capacities, in particular the capacities of data protection authorities in monitoring cross-border data transfers and enforcement of relevant laws and regulations in cases of breaches or misuse.

The proposed Framework will embrace state-of-the-art technologies and be respectful of countries' laws and regulations. Governments are not obliged to use specific technologies. The use of open standards and norms will guarantee a large diversity of technological choices by the States while facilitating country ownership and interoperability.

2. INTRODUCTION

In 2020, AU Member States adopted the Digital Transformation Strategy (DTS) for Africa (2020-2030) with the vision of establishing:

An Integrated and inclusive digital society and economy in Africa that improves the quality of life of Africa's citizens, strengthen the existing economic sector, enable its diversification and development, and ensure continental ownership with Africa as a producer and not only a consumer in the global economy.

Realising this ambition – as well as that of the AfCFTA – depends on the development of inclusive and trusted foundational digital ID systems that enable all African citizens to prove and verify their legal identity reliably and securely when transacting in-person and online, and enable public and private sector service providers to recognise identity credentials, no matter where in Africa they have been issued. Importantly, foundational digital ID systems must be designed to empower people, especially disadvantaged and marginalised populations. This will enable all African citizens to meaningfully participate in the digital economy and society, unlock access to services within countries and across borders, promote trade as part of the AfCFTA, enhance trust in the digital society and economy, and reduce fraud and costs of doing business in and with Africa.

Importantly, foundational digital ID systems can also underpin the development of broader 'digital stacks'[23] with digital payment and trusted data sharing platforms to create opportunities for innovation and a wide range of presence-less, paperless and cashless transactions across the continent. However, this also requires risks related to exclusion, data protection, cybersecurity and technology, and vendor lock-in to be comprehensively mitigated. It is for these reasons that digital ID is one of five cross-cutting themes of the DTS, providing the mandate and setting for this Framework.

2.1. VISION, OBJECTIVES AND INDICATIVE USE CASES

The vision of the AU Interoperability Framework for Digital ID is that all African citizens in Africa can easily and securely access the services they need, when they need them, from both public and private sector providers, which will encourage inclusive and meaningful participation in the wider digital economy and society and allow services to operate with greater trust and certainty.

To this end, the Framework defines common requirements, minimum standards, norms, governance mechanisms, alignment among legal frameworks with the objectives to:

23 In the context of digital technologies, a 'stack' is a collection of independent software components or infrastructure that work together to support the execution of a use case.

1. allow all African citizens to **verify their legal identity offline and online** to access public and private sector services in all participating AU Member States thereby contributing to achieving accelerated progress towards continental unity and integration for sustained growth, trade, exchanges of goods, services, free movement of people and capital through establishing a united Africa and fast-tracking economic integration through AfCFTA as stated in aspiration 2 of the Agenda 2063;

2. empower all African citizens with **control over their personal data**, including the ability to selectively disclose only those attributes that are required for a particular transaction. The personal information to be disclosed should be minimal, proportionate and should contain only the information relevant to that particular transaction; and

3. strengthen **trust and interoperability** among foundational identification systems of AU Member States.

The Framework does not call for the creation of a unified continental digital ID system but provides a foundation for interoperability between existing digital ID systems of AU Member States that takes into consideration the digital sovereignty of AU Member States, the differences in the digital infrastructure rollout, the availability of associated policies and regulations, and the vulnerability of populations during and after the implementation of digital ID systems.

It is paramount that this Framework is developed in line with best practices and international norms[24] aimed at protecting personal data, maintaining cybersecurity, and safeguarding people's rights. With the adoption on the Malabo Convention,[25] the AU has taken an important step towards establishing a credible digital environment for online transactions via the adoption of a common set of rules to govern the cross-border transfer of personal data across the continent and the alignment of national data protection and cybersecurity frameworks.

A continental Framework can facilitate **access to services in all participating countries by enabling people and businesses** to verify credentials and other facts without disclosing personal data. This includes the possibility to authenticate identity when accessing online services (e.g., government services) in another country with their digital ID without the need to enrol in the local foundational identity solutions recognised by foreign service providers. The interoperability of digital ID also facilitates the sharing of and consent for verifiable credentials and trusted data when applying for services where the law demands such verification (e.g., proof of insurance, qualification vaccination status); enabling people to save time and reduce red tape.

24 This includes among other policy instruments, the Convention on Cybercrime of the Council of Europe (CETS No.185), known as the Budapest Convention on Cybercrime, see: https://www.coe.int/en/web/cybercrime/the-budapest-convention; ISO/IEC 29151, see: https://www.iso.org/standard/62726.html; the UN Principles and Recommendations for Vital Statistics Systems, see: https://unstats.un.org/unsd/demographic/standmeth/principles/m19rev3en.pdf; international norms on data protection (such as the GDPR and Council of Europe Convention 108+); global and regional standards and trust frameworks for identification.

25 AU (2014) Convention on Cyber Security and Personal Data Protection, see: https://au.int/en/treaties/african-union-convention-cyber-security-and-personal-data-protection.

It can also **enhance the integrity and accessibility of cross-border payments and financial services in Africa, and create opportunities for innovation**. Weak and untrusted ID systems, coupled with the absence of harmonisation of rules, create anti-money laundering/combating financing of terrorism (AML/CFT) risks,[26] which introduce barriers to cross-border exchanges, raise costs of services (e.g., remittances), and hamper innovation. Digital ID can facilitate customer identification and verification at on-boarding, support KYC processes, and aid the monitoring of transactions for the purpose of detecting and reporting suspicious transactions. Interoperability will not only make it easier for migrants to send money home by easing the KYC verification and the authentication burden, it will also help to lower costs, helping Africa to move closer to the SDG target (10.c) of three percent by 2030.

A continental Framework can also **strengthen trade and e-commerce by increasing trust in online commercial transactions and making it easier to do business and trade across Africa**. In 2020, intra-African trade represented approximately 16.6% of 'Africa's GDP.[27] The AfCFTA was launched in 2019 to unlock new opportunities for trade and e-commerce by 2030. Cross-border recognition of digital IDs can aid stronger identity checks of buyers and sellers, especially for restricted goods sold online. It can also enable e-signatures for online, paperless transactions, which enable businesses and clients to save time and increase security by reducing risks of identity fraud. It also simplifies doing business across borders by enabling businesses to digitally manage their interaction with the government, such as declaring tax, participating in procurement procedures, requesting VAT numbers, and applying authorisations.

2.2 SCOPE

To achieve these objectives, the Framework will define:

- the **type of information/data** that can be shared in the form of a minimum dataset for foundational identity information;[28]
- the **way of proving who issued the data** and that it can be trusted by;
  - establishing a process to communicate trusted authoritative sources[29] for identity data in each AU Member States; and
  - determining how to verify the authenticity of the digital claim; as well as
- the standards and processes that describe how data is shared by users and verified by others in offline and online environments.

26 AML/CFT risks refer to anti-money laundering and counterterrorist financing risks. The Financial Action Task Force (FATF) recommends to governments that they develop an integrated multi-stakeholder approach to understanding opportunities and risks relevant to digital ID and developing regulations and guidance to mitigate those risks.

27 AML/CFT risks refer to anti-money laundering and counterterrorist financing risks. The Financial Action Task Force (FATF) recommends to governments that they develop an integrated multi-stakeholder approach to understanding opportunities and risks relevant to digital ID and developing regulations and guidance to mitigate those risks.

28 Although the scope of this document focuses on identity data, the proposed Trust Framework can be extended by AU Member States to represent other proofs and achievements, such as diplomas, professional qualifications, etc.

29 Member States will maintain legal responsibility and accountability relative to the trusted authoritative sources (data issuers).

This document outlines the foundations of a trust and interoperability framework for digital ID systems across the African continent. It will define the minimum requirements necessary to ensure interoperability between existing and future digital ID systems. Interoperability refers to the ability of different parties of the Framework – such as digital ID systems and the systems of relying parties – to communicate and interface effectively at technical and semantic levels. Interoperability can facilitate mutual recognition, which is a legal construct, but is not a prerequisite, and nor does it guarantee mutual recognition. The Framework does not define a unified digital ID system for Africa and does not address commercial and liability agreements between participating Member States.

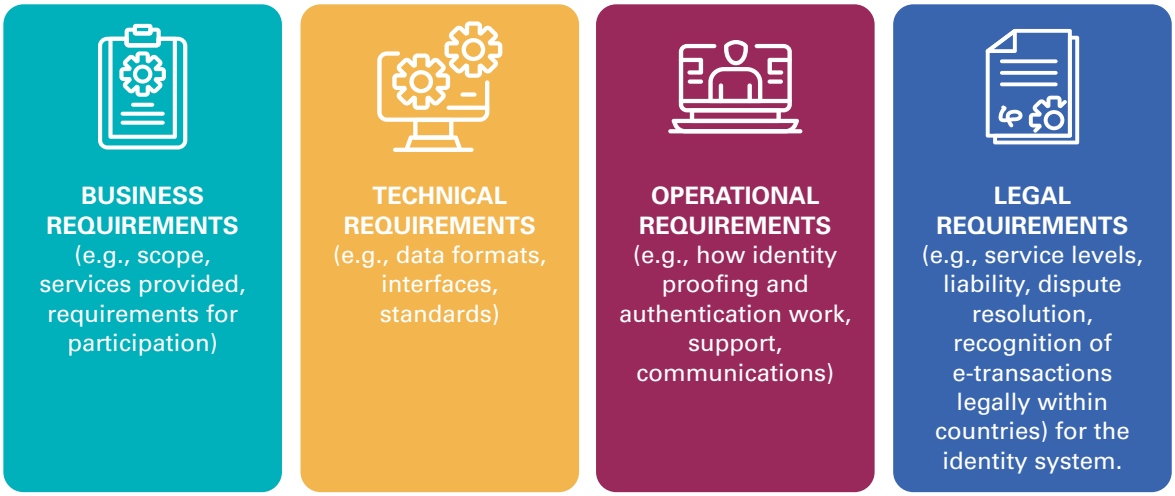
Many African countries already have digital ID systems well underway, and some have introduced digital authentication capabilities. **The Framework provides common requirements for communicating foundational identity data and processes that would be interoperable and accepted in other African Member States, while Member States retain full control and choice for the design of their national systems.**

The Framework complements and builds on, rather than duplicate activities associated with the Protocol to the *Treaty Establishing the African Economic Community Relating to Free Movement of Persons, Right of Residence and Right of Establishment, and the Conference of African Ministers Responsible for Civil Registration and the African Program for Accelerated Improvement of CRVS* (APAI-CRVS). Implementation of the Framework should be closely coordinated with this and other relevant initiatives, such as to explore migration as an additional use case for digital IDs at the appropriate time and to ensure that the coverage and quality of CRVS systems are improved as an important input for digital foundational ID systems.

2.3. TRUST FRAMEWORK, DATA PRIVACY, INTEROPERABILITY AND STANDARDS

Identity systems should foster trust between the various participating parties, ensuring that the legal rights of both individual users and operating agencies are observed, and that the ethical use of identity systems is promoted. **To ensure this trust, a set of rules that all parties sign up to and observe** must be defined; a Trust Framework.

Whilst technology acts as a key enabler, Trust Frameworks also focus on process and procedure. A robust Trust Framework should clearly define the:



The Framework is based on **interoperability**. To facilitate interoperability, one entity must be able to trust another entity based not only on the integrity of technical processes (e.g., cryptographic proof, etc.), but also regarding the provenance of the data being shared (e.g., the processes for its collection and for attributing a certain record to an individual).

Interoperability does not require that foundational ID systems be uniform, but simply that certain common and open standards are followed. Under the Framework, each participating country can create foundational ID systems adapted to their local needs, traditions, and legislation, as long as certain standards that enable interoperability are followed. Open **standards** establish universally understood and consistent interchange protocols, testing regimes, quality measures, and good practices regarding the capture, storage, transmission, and use of legal identity data, as well as the format and features of legal identity credentials and authentication protocols.

When considering interoperability of digital ID credentials and authentication across the continent, it will be important to consider open standards for the identity claims, how they are issued, and how trust is communicated between the entities involved in the Trust Framework. These claims, which will form the **basis for legal digital ID**, will often originate from authoritative sources such as government agencies. An authentication mechanism must also be defined to enable legal digital ID holders to share these claims with services providers appropriately, ensuring that disclosure of data is binary and any metadata is anonymous, as well as the privacy and rights of individuals protected at all times.

This framework will define **how the trust can be established in these verifiable claims, and how governance elements and standards for data operate**. The technical implementation of the solution can be driven by the market, which will be able to leverage the Trust Framework to develop innovative digital foundational ID solutions. The Framework places data privacy, auditing and data protection at the centre and lays a transparent procedure to apply to all involved relying parties on how data is requested, gathered, transmitted and stored. It follows well-accepted standards on information/data sharing procedures. The importance of tokenisation for reducing opportunities for data harvesting, cloning and fraud (by presenting the ID holder with the functionality to issue virtual IDs in order to protect the actual IDs themselves), is an additional aspect that will be further elaborated to strengthen data privacy at national/continental level.

3. THE FRAMEWORK

The AU Interoperability Framework for Digital ID proposes to define, at the continental level, a harmonised approach for individuals to share digital ID claims[30] issued by trusted authorities with service providers in order to prove their legal identity in an online and offline environment. It will consist of agreeing on a **common standard to represent existing proofs of legal identity issued by AU Member States in a digital format.**[31] The authenticity of such credentials[32] would be able to be verified in order to guarantee a high level of trust and security.

There are no restrictions placed on national foundational identity systems, how they operate or which types of credentials they use to authenticate individuals; each country is sovereign in this respect. The Framework intends to create conditions for interoperability at a continental scale, building on and extending the reach of existing systems where they exist, rather than restricting their use.

The interoperable digital ID credentials (IDC-ID) issued in line with the Framework will take the form of a verifiable claim that will be complementary to existing national foundational ID systems and regional cooperation projects, without replacing the domestic digital identification systems of AU Member States. **AU Member States remain free to select how they want to issue this digital credential.** It may be stored in a purely digital format on a smartphone application, a cloud-based server, a smartcard, or a link to the digital representation may be established using a one- or two-dimensional barcode on a paper document (printed on paper, plastic card).

The Framework is based on the development of interoperable, inclusive and trusted ID systems as these provide the backbone of authoritative sources of data on people's legal identity and thus enable the IDC-ID to achieve higher levels of assurance. AU Member States are therefore encouraged to strengthen their ID systems, potentially drawing upon the *Principles on Identification for Sustainable Development*.[33] Alternative solutions to obtain an IDC-ID for people that are currently excluded from an ID system can be considered.

The standards for an interoperable legal digital ID could be used at the domestic level or support cross-border use cases. For example, the standard could be adopted to:

- represent foundational digital ID data at the national level on newly issued or updated digital ID credentials; or
- represent foundational digital ID data at continental or REC level; or
- be issued separately to complement to pre-existing foundational digital ID systems.

30 'Claims' are a collection of attributes about a data subject: e.g., family name or date of birth. A 'verifiable claim' is a tamper-evident version of this information which can be cryptographically verified in order to check its authenticity.

31 The current framework focusses on the definition of verifiable claims to prove identity data but could be expended to share verifiable claims about academic achievements, professional qualifications, etc.

32 A 'credential' is composed of an identity claim, metadata about the issuer, and a proof of authenticity, which is usually a digital signature.

33 The Ten Principles on Identification for Sustainable Development have been endorsed by 30 international and regional organisations, including African institutions such as UNECA, AfDB and Smart Africa, as well as adopted by a number of African countries. See: https://id4d.worldbank.org/principles.

The interoperability, trust, and inclusivity elements defined as part of this framework constitute a launch pad for a more comprehensive continental framework and infrastructure for digital identification and authentication on the continent.

3.1. GUIDING PRINCIPLES

The following principles shall guide the cross-border interoperability implementation of the Framework:

1. Transparency in governance and operation.
2. Easily accessible, cost-effective, operationally sustainable, and widely usable.
3. Promote, respect, and uphold human rights and freedoms.[34]
4. Ensure technical integrity, including unique, secure, scalable, and accurate identity.
5. Guarantee the sovereignty of Member States, ensuring data sovereignty. Notably, digital ID data belongs to, and remains in the control of Africa.
6. Be interoperable among AU Member States.
7. Use open standards[35] and prevent vendor and technology lock-in.
8. Protect data privacy and enable people to control their personal data, including data proportionality through system design.
9. Safeguard data privacy, security, and rights through a comprehensive legal and regulatory framework.
10. Establish clear institutional mandates and accountability.

Considering that the Framework depends on authoritative sources, such as legal identification systems, the quality and coverage of these systems therefore has an impact on its implementation. Exclusion from these systems and other challenges such as weak security, for example, will lead to the same in terms of the ability to issue and properly use credentials.

Therefore, AU Member States should meet their obligations to ensure that all people present in their territory have access to legal identification, in line with the Convention on the Rights of the Child and other international and regional legal instruments. Furthermore, they are also strongly encouraged to adhere to existing relevant international norms[36] and principles[37] and ensuring that authoritative sources, and especially their legal identification systems, are inclusive, protective of people's data and rights, and designed to support the continental economic and societal integration.

34 As per the African (Banjul) Charter on Human and Peoples' Rights (Adopted 27 June 1981, OAU Doc. CAB/LEG/67/3 rev. 5, 21 I.L.M. 58 (1982), entered into force 21 October 1986).

35 'Open standards' are standards made available to the general public and are developed (or approved) and maintained via a collaborative and consensus driven process. Open standards facilitate interoperability and data exchange among different products or services and are intended for widespread adoption (adopted from ITU-T).

36 This includes among other policy instruments, the Convention on Cybercrime of the Council of Europe (CETS No.185), known as the Budapest Convention on Cybercrime, see: https://www.coe.int/en/web/cybercrime/the-budapest-convention; ISO/IEC 29151, see: https://www.iso.org/standard/62726.html; the UN Principles and Recommendations for Vital Statistics Systems, see: https://unstats.un.org/unsd/demographic/standmeth/principles/m19rev3en.pdf; international norms on data protection (such as the GDPR and Council of Europe Convention 108+); global and regional standards and trust frameworks for identification.

37 Such as the Ten Principles on Identification for Sustainable Development, which have been endorsed by 30 international and regional organisations, including African institutions such as UNECA, AfDB and Smart Africa, as well as adopted by a number of African countries. See: https://id4d.worldbank.org/principles, and the Principles on Digital Development, which have been endorsed by 200+ organisations, see: https://digitalprinciples.org/.

3.2. THE MODEL

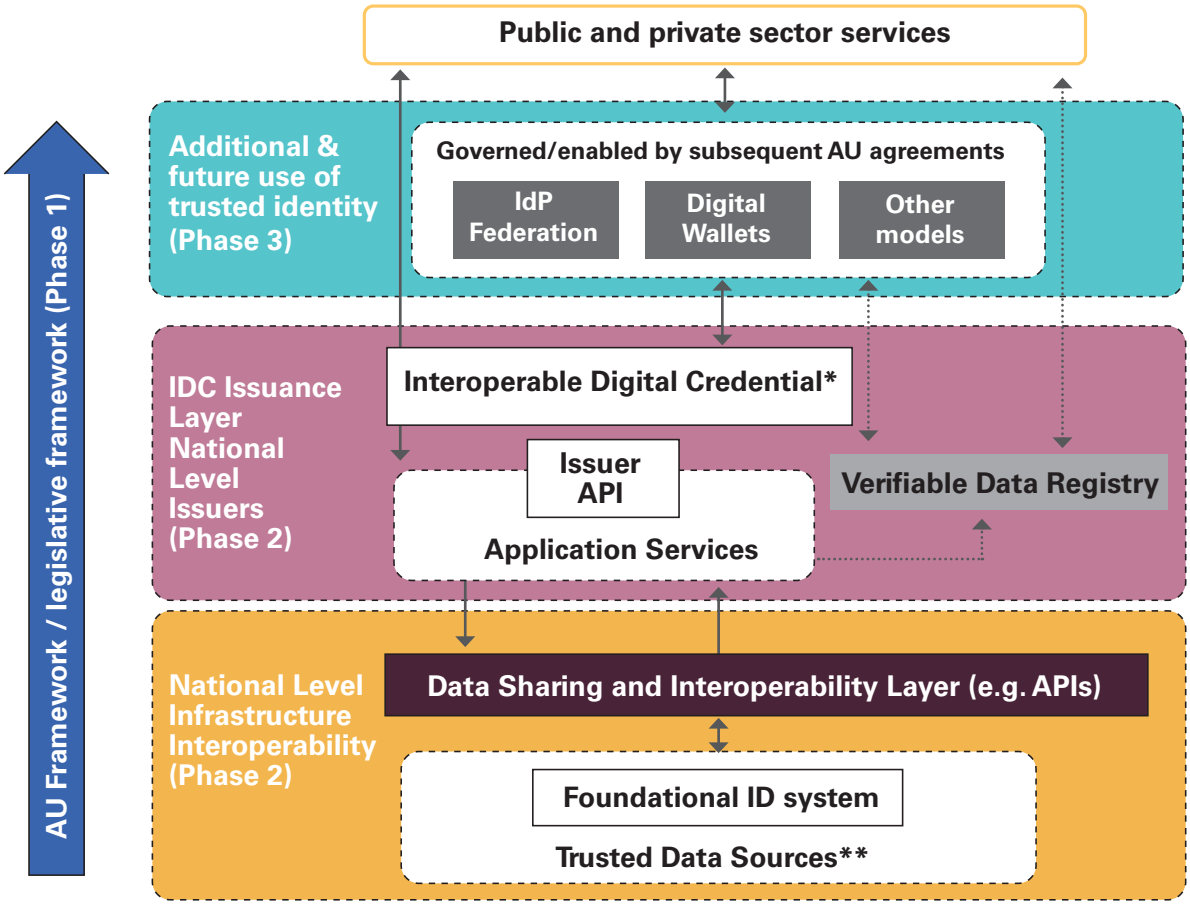
The Framework proposes implementation in three phases:

1 Adoption of the Framework and development of an enabling legislative framework.

2 Implementation of the framework and adoption of technical specifications for the IDC-ID.

3 The scale-up of the implementation of the framework and the provision of an infrastructure that enables more advanced use cases such as remote authentication.

FIGURE 1 – PHASED IMPLEMENTATION APPROACH TO THE FRAMEWORK



* *Implementation details of phase 2 will be further discussed with AU Member States.*

** *Member States will decide what trusted data sources entail their foundational ID systems.*

The IDC-ID shall ensure that **issuing authority does not know which services individuals access with their digital ID,** but authenticity of the identity credentials can be checked. This provides safeguards in terms of data protection and privacy, and also gives more control to the individual on how his or her data is used.

The infrastructure layer will enable more advanced use cases and will operate by binding identity credentials issued in the IDC-ID format to the actual individuals. Several technical options are available to AU Member States to implement this layer, including a federation of identity providers providing authentication mechanisms to the holders of the IDC-ID, or the development of digital ID wallets solutions, or any other models enabling interoperability. Each of these implementations can **offer data minimisation and selective disclosure services** for specific use cases, for example by only sharing the relevant data points from an ID card and credit report to obtain a loan, seek social or health benefit, obtain a pension benefit, apply for scholarships, or anonymise the IDC-ID minimum dataset (name, date of birth) into a proof of majority (+18y or +21y or a yes/no response).

3.2.1. ARCHITECTURE COMPONENTS

Trusted data sources must meet standards set by the Framework for data quality and integrity. In many cases, this would be fulfilled by a foundational ID system (whose trusted data sources will be decided by Member States) that can provide a proof of legal identity.

Figure 1 depicts the extending of access to existing national systems and trusted data sources through a data sharing and Interoperability layer based on standards and protocols enabling trusted IDC Issuance. Services providers will be required to verify and retrieve legal identity data when creating foundational digital ID credentials.

The IDC Issuance Layer depicts the standardised issuance of IDC credential based on a foundational/national level ID system trusted data source. Each credential Issuer (at least one per participating member state) will have a number of key functions (not limited to the following):

- An Issuer API that enables wallets and other systems to request and retrieve credentials;
- A Verifiable Data Registry that enables the verification of identifiers and credential revocation checking;
- Cryptographic Key Management;
- Visibility and Auditability of credential use for the holder of an IDC credential;
- Providing Credential Metadata alongside each issued credential to describe the quality, provenance, and level of trust associated with the issued credential.

3.2.2. NATIONAL LEVEL AND INTEROPERABILITY REQUIREMENTS

There is no requirement for existing identity systems at the domestic level to be re-engineered to achieve interoperability at the continental level. Instead, standards for data interoperability, technical interoperation via application programming interfaces (APIs) and protocols, and the technical representation of credentials will be adopted. The issuance of credentials and their creation is separate from existing national systems but would be under the control of nationally responsible agencies.

Technical trust, underpinned by advanced cryptography, may not require a continental PKI or other super-national infrastructure, but would instead stem from AU Member State preference and/or capability; utilising either national PKI (where used) or legally recognised alternatives. Each AU Member State will continue to exercise national sovereignty in the design of national identity systems, including how those systems interoperate with the AU Framework.

3.2.3. STANDARDS FOR THE PARTICIPATION OF TRUSTED DATA SOURCES

Standards will be set under the Framework for the quality, security, reliability, and minimum level of assurance associated with each trusted data source. Member state systems should provide evidence that they have reached the minimum requirements for participation before they are able to participate in the Framework and issue IDC-compliant credentials. The nature of these standards will be determined by agreement of the AU member states.

3.3. TRUSTED PROCESS – THE TRUST FRAMEWORK

The Trust Framework should describe clear rules for the participation of entities (e.g., issuers, holders, and verifiers of identity), the operation of the Framework, and the technical requirements for interoperability of trusted credentials.

This will enable all entities to trust the credentials shared by holders of identity based on the trust established by the issuing authority (for the credential) and the processes each entity has agreed to adhere to under the Trust Framework.

It is expected that the following key sections would be drafted by the Member States as part of the Trust Framework.

3.3.1. ROLES AND RESPONSIBILITIES

A clear definition of each entity (e.g., an issuer of credentials), and the responsibilities it has for trust to be maintained, such as the safe and secure management of data and services, and incident reporting.

Key roles expected to be included in the Trust Framework would be that:

- The **trusted authorities** are authoritative sources of data for legal proof of identity as endorsed by AU Member States.
- The **issuers** are entities responsible for issuing the proof of legal identity in the standardised digital format under the Framework to the holder. Trusted authorities can either issue the credentials themselves or mandate another entity with a more adequate skillset (e.g., ICT agency, private sector).
- The **holder** of the IDC-ID is the individual that possess one or more digital credentials. The holder can (but not always) be the subject of the identity attributes shared via the IDC.
- The **verifier** is a relying party (e.g., public or private service provider) that wants to verify the identity claim of a given subject.
- **Identity providers, credential providers**, and digital wallet providers can further contribute to the ecosystem by providing an authenticator to bind the identity of the holder to the credentials and therefore enable more advanced use cases requiring remote authentication.

An independent Supervisory Body to be established by Member States may be necessary to ensure that participating entities remain compliant with the rules laid down by the Trust Framework and set minimal tools and technologies required for compliance. The Supervisory Body should also be entrusted with the task of raising awareness of cyber resilience skills across the continent to ensure the sustainability of the Framework.

3.3.2. RULES FOR PARTICIPATION

Rules for participation may include minimum legal, operational, or organisational requirements required for a trusted authoritative entity providing a service under the Trust Framework. For example, an Issuer may be required to have official authorisation to operate (from an authoritative source / government agency).

Services accepting IDC-ID may be requested to confirm their conformance with baseline data protection, privacy, and redress (for identity holders) requirements.

An MoU may also be required to ensure that all operating entities agree with the terms of the Trust Framework.

3.3.3. GOVERNANCE

Governance mechanisms to be endorsed by AU Member States will be required to set and maintain the rules of the Trust Framework, approve changes to the interoperability requirements, and to delegate responsibility for the drafting/development of changes to the Framework to governance sub-groups as necessary.

An Independent Supervisory Body to be established by AU Member States may be necessary to ensure that participating entities remain compliant with the rules laid down by the Trust Framework. This entity should also be responsible for ensuring that all parties satisfy formal compliance to standards and, should they deviate, are audited or brought to account as deemed necessary, for example, in the case of a data breach.

The protection of individuals should be paramount. The Supervisory Body should be empowered to receive and act upon complaints by IDC-ID holders affected by poor practice, data breaches, identity fraud, or other incidents related to digital ID. It should also be the focal point for mechanisms of redress even if this is only a coordinating role and should act as a champion of individuals and their rights.

3.3.4. INTEROPERABILITY REQUIREMENTS

3.3.4.1. LEVELS OF ASSURANCE

A means of communicating the level of trust in a credential presented by a holder to a verifier. The Framework should define the conditions by which each level can be achieved based on the verification of identity by an authoritative source, the issuance process, and the means of holding and presenting a credential.

3.3.4.2. MINIMUM DATASET

The minimum amount of data regarding the identity of a holder as provided in an identity credential, should be adequate for the identification of the individual in the majority of common transactions whilst respecting the need for data minimisation. Attributes contained in the minimum dataset can be provided by different trusted entity.

The governing body is at liberty to define how additional claims (datasets) may be included optionally in the Trust Framework. Any issuance of corresponding credentials should be subject to the same conditions and rules as issuers of foundational identity credentials.

3.3.5. TECHNICAL REQUIREMENTS

3.3.5.1. SECURITY

Baseline security requirements should be defined for each entity providing a service as part of the identity infrastructure.

3.3.5.2. CRYPTOGRAPHIC PROOF

Credentials will be verified by the inclusion of a digital signature created by the issuing authority. Checking the validity of the signature acts as cryptographic proof that the claim made by the holder presenting the credential can be trusted. To check, a digital signature public key will be required. The public key may be provided through a decentralised or centralised method to be determined as part of the Trust Framework and its technical requirements.

3.3.5.3. CREDENTIAL FORMAT

Technical specifications for the creation and transmission of credentials should be defined, drawing on existing standards such as W3C Verifiable Credentials where applicable.

The **Interoperable Digital Credential for Identity** (IDC-ID) is a set of legal identity claims (e.g. attributes) and relationship made by an issuer that can be cryptographically verified. More specifically it includes:

- Credential metadata about the type of credential issued, date of issuance, and name of issuer;
- Information about the subject of the claim and the actual legal identity claim (e.g., date of birth);
- Proof of authenticity, which is usually a digital signature.

The holder of the IDC-ID is able to generate **verifiable presentations** of one or more IDC-ID in the way that the authenticity of the claim can still be verified (e.g., selective disclosure)

3.4. POTENTIAL AUTHENTICATION OPTIONS

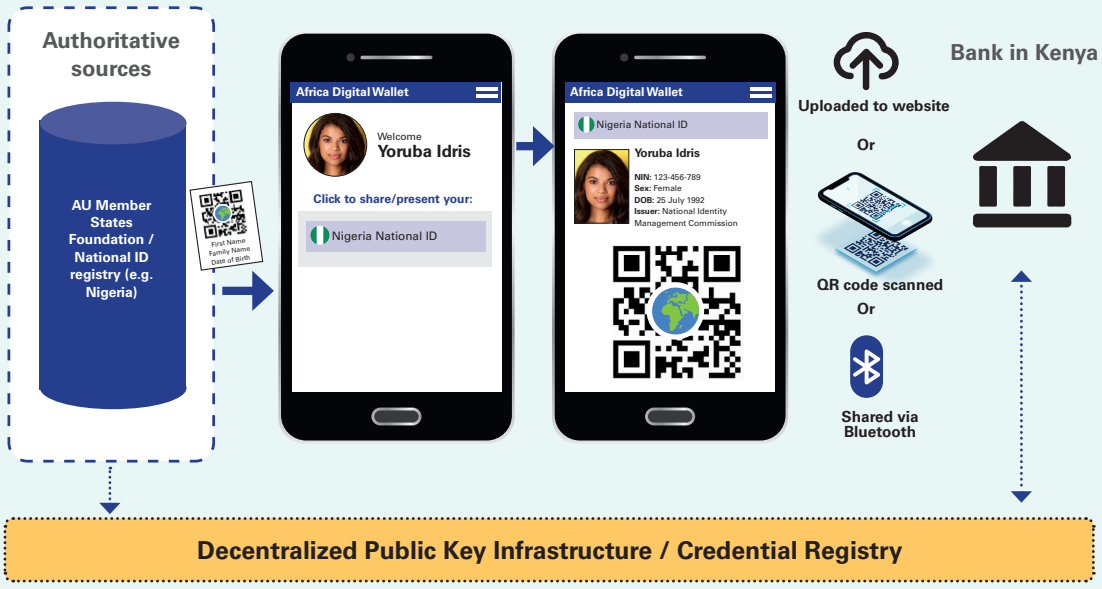
Several architectural approaches can be adopted to enable the holder of IDC-ID to be authenticated at a given level of assurance. The following options can co-exist and be implemented at different levels of cooperation (e.g., among specific sectoral actors or at the REC level).

Depending on availability of other technologies with proven implementation practices, additional options may be explored.

3.4.1. OPTION 1 - PERSONAL DIGITAL WALLETS

This option provides individuals and businesses with a personal digital wallet containing verifiable proof of legal identity attributes that can be used to prove one's identity or share specific facts with a service provider. This architecture option refers to W3C Verifiable Credentials Use Cases.[38]

FIGURE 2 – OVERVIEW OF OPTION 1 - PERSONAL DIGITAL WALLETS



AUTHENTICATION PROCESS

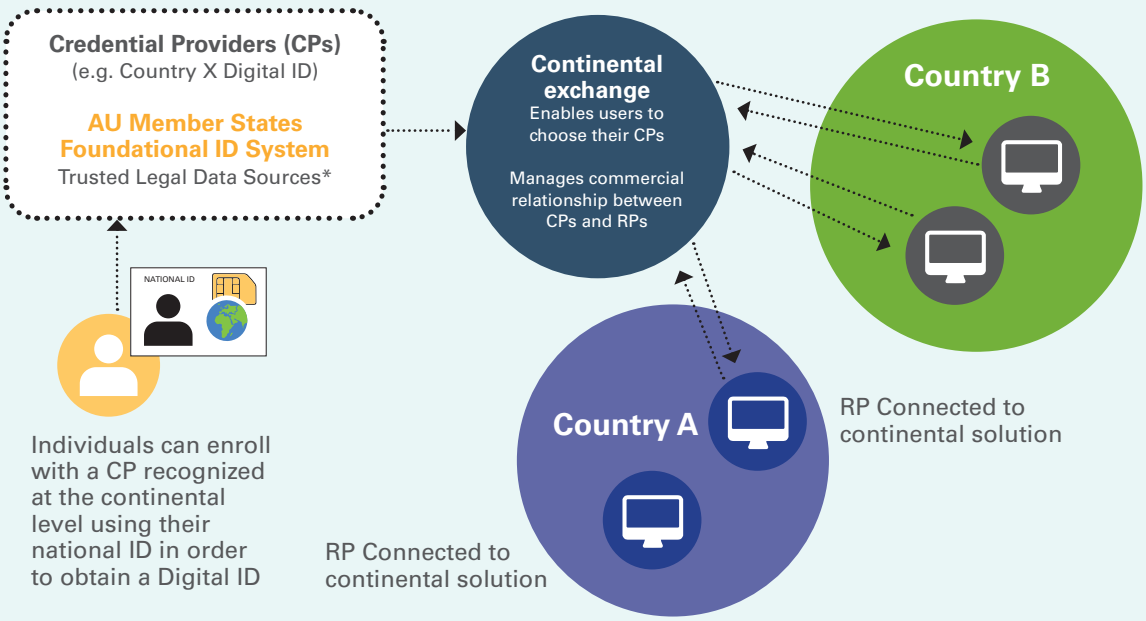
1. Individual selects an **identity wallet provider** to store his/her IDC and an onboarding process is necessary.
2. The individual receives a verifiable IDC (e.g., ID, proof of address) from the authoritative source issuers and stores it in a **digital wallet.**
3. At the same time of the issuance, the authority records a digital print of the claim in a **decentralised public key infrastructure, taking into account citizens' privacy.**
4. The individuals can present to a service provider (e.g., an insurance) a claim such as a **proof of address**, using his/her wallet (by QR code, Bluetooth, NFC).
5. The service provider can use the decentralised public key infrastructure to verify that the claim is authentic and has been issued by a recognised authority.

38 W3C (2019) Verifiable Credentials Use cases, see: https://www.w3.org/TR/vc-use-cases/.

3.4.2. OPTION 2 - CONTINENTAL DIGITAL ID FEDERATION

Under this model, each African resident would be able to onboard with a continental-level credential provider of their choice.

FIGURE 3 – OVERVIEW OF OPTION 2 – CONTINENTAL DIGITAL ID FEDERATION



* Member States will decide what trusted data sources entail their foundational ID systems

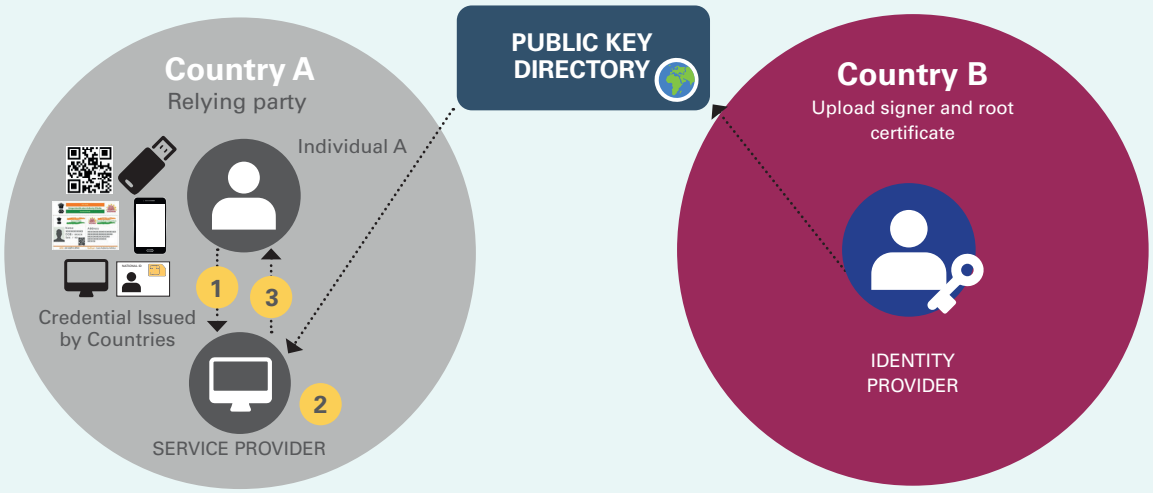
AUTHENTICATION PROCESS

1. A **continental federation of ID credential providers is established**: telecom operators, banks, governments, etc., can provide authentication services.
2. A **continental exchange** is created, providing a single point of contact for all the participating credential providers and relying parties that want to authenticate individuals.
3. Individuals can use their IDC issued by an authoritative source (e.g., legal identification system) to onboard to the credential provider of their choice. The credential provider can verify the authenticity of the IDC.
4. Upon successful verification, the credential provider issues **an authentication means** to the individual.
5. The individual can use his or her authentication means to **access online and in-person services** that are connected to the continental exchange.

3.4.3. OPTION 3 - DIGITALLY SIGNED CREDENTIALS

This model enables authentication by verifying the digitally signed legal identity data on a credential with a public key, as well as an additional means to share the holder's picture.

FIGURE 4 – OVERVIEW OF OPTION 3 - DIGITALLY SIGNED CREDENTIALS



AUTHENTICATION PROCESS

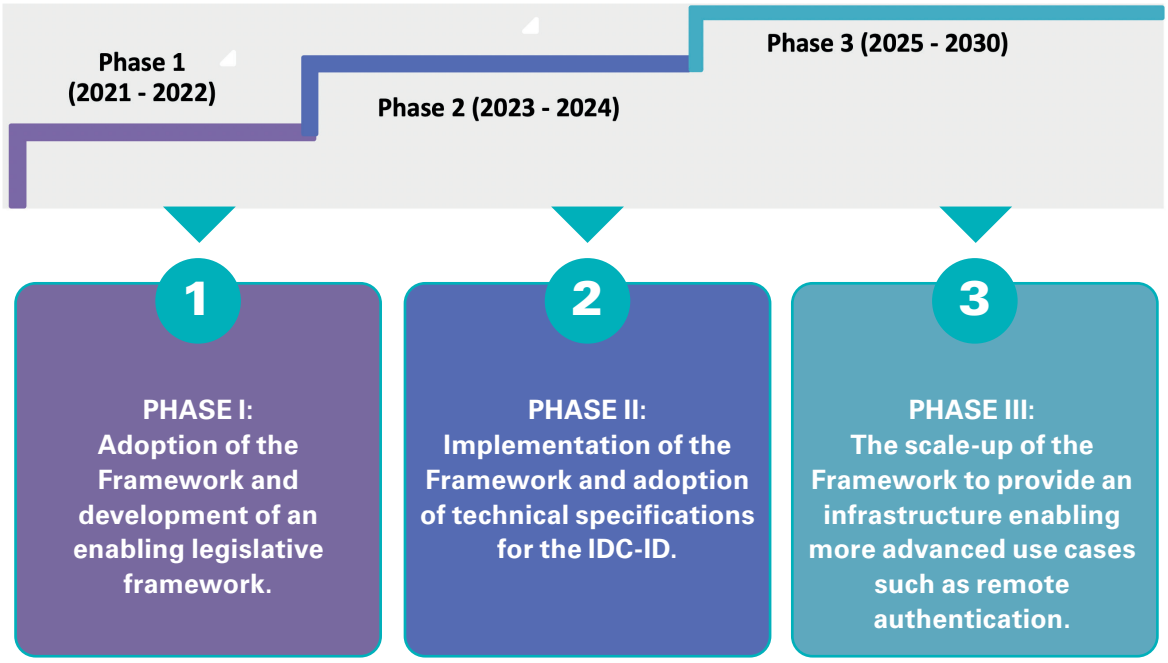
1. **Countries agree on a standard** (e.g., a QR code) and authoritative sources cryptographically sign credentials (via a private key).
2. **Authoritative sources share their public key** in a Public Key Directory (PKD) whose governance will be endorsed by AU Member States and managed at the continental level.
3. **Countries create a separate service** enabling to share a copy of the picture of the IDC-ID holder accessible via secure API in order to authenticate the holder. To work offline, it is also possible for a group of countries (e.g., RECs) to agree on the issuance of a physical credential containing a picture of the holder.[39]
4. **Countries authoritative sources** issue standardised forms of IDC to individuals.
5. **A verification software (app or website) is created** to enable service providers to verify the authenticity and integrity of the signature on the IDC.
6. **Individuals can use their IDC to get their legal identity** digitally verified by public or private relying parties in their country or abroad and access services.
7. **Each Member State will be expected to maintain the private keys**, root certificates and hashing algorithms in secure storage such as Hardware Security Modules (HSMs) for encryption and integrity checking.

39 The issuance of physical credentials comes at an additional cost. Participating Member States would have to discuss further the financing of such solution in order not to create barriers to access.

4. HIGH-LEVEL ROADMAP FOR IMPLEMENTATION

To accelerate the path towards achieving the ambitious objectives of this Framework, AU Member States should increase their collaboration to refine the details of the technical and reference framework, common standards, and processes.

The proposition is to divide the implementation of the Framework in three phases, as shown in the diagram below:



For each phase, opportunities for consultation with AU Member States, civil society, and other stakeholders of the identity ecosystem will be planned to ensure that the Framework and implementation remain aligned with the needs of the individuals and local contexts. Key documentation will be published and ample time will be provided for contributions and consultations.

4.1. PHASE 1: ADOPTION OF THE FRAMEWORK AND ENABLING ENVIRONMENT

Submission of the draft Framework to the 4th ordinary session of the STC on communication and ICT for adoption and the endorsement by policy organs.

Following the endorsement of the present document, the details of the Trust Framework will be further specified and the following activities will be conducted notably:

- awareness creation;
- feasibility study on the current landscape of the digital ID system in Africa;
- establishment of a consultation framework for digital ecosystem actors aimed at safeguarding the interest of each actor;
- development of harmonised legal and regulatory instruments;
- definition of the rules for participation;
- establishment of the governance mechanisms and forum to share best practices throughout the implementation process;
- defining legal provisions that will need to be integrated in domestic legal environments of AU Member States in order to implement the Framework, including appropriate safeguards on cybersecurity and data protection;
- ratification of the Malabo Convention on Cybersecurity and Personal Data Protection;
- adoption of the continental data policy framework;
- nomination of expert groups by AU Member States to define the interoperability and technical requirements;
- establishment of an independent institutional structures at national level (data protection authorities; controller of certifying authorities; and computer incident response teams (CIRTs) and strengthen cooperation among national institutions;
- develop capacity building initiatives;
- support the rollout of digital infrastructure, including data centres at national, regional/continental level, that are required to support and sustain the operationalisation of the digital ID systems; and
- resource mobilisation.

In order to ensure the success of the Framework, a series of **use cases** representing a range of opportunities for the continent will be defined. A group of AU Member States can further collaborate to test and pilot specific use cases, along with additional stakeholders as needed.

An assessment of the **major costs and benefits** of the proposed framework and subsequent authentication options should be conducted in order to provide more visibility on the financing needs and inform AU Member States decision-making. It is currently expected that compliance with a harmonised standard to represent identity information will engender limited costs for AU Member States as it could be integrated as a technical requirement to existing digitalisation projects of Member States' foundational ID systems. However, the establishment of the authentication infrastructure is expected to generate additional costs and depending on the types of stakeholders involved, require the definition of business models. For this phase, a detailed impact assessment will have to be performed in order to ensure that the authentication options proposed remain inclusive.

In parallel, AU Member States commit to:

- developing and implementing harmonised and enabling legal and regulatory frameworks that build trust in digital foundational ID systems;
- developing harmonised personal data legislation and regulation that empower individuals, while maintaining data sovereignty;
- rollout digital infrastructure including data infrastructure (national data centres) which is the base for rolling out the digital ID system;
- ratify of the *AU Convention on Cyber Security and Personal Data Protection (if not done so far)* and expedite its entry into force and work to accelerate the establishment of data protection authorities for oversight in participating countries;
- developing the national cybersecurity strategy and establishing computer incident response teams (CIRTs) to mitigate risks and threats related to cyberattacks, data robbery and mishandling of sensitive information;
- adopting the AU continental data policy framework; which calls for digital ID systems to be constructed and implemented cohesively in line with this overarching data governance framework that ensures that the combination and repurposing of public administrative data entailed by digital identification systems is done with appropriate safeguards. These should empower the individuals and protect online privacy as a fundamental right (to include user choice and control, informed/meaningful consent, data sovereignty/ownership, etc.);
- launching and/or scaling up efforts to strengthen foundational ID systems, and to ensure that they are inclusive and trusted, in line with relevant norms and initiatives such as the African Programme for Accelerated Improvement of Civil Registration and Vital Statistics Systems (APAI-CRVS) and the *Principles on Identification for Sustainable Development.* This phase will be finalised with the adoption of the completed version of the Framework by AU Member States.

4.2. PHASE 2: IMPLEMENTATION OF THE FRAMEWORK AND ADOPTION OF TECHNICAL SPECIFICATIONS FOR THE IDC-ID

The second phase will consist of establishing the Trust Framework governance and cooperation mechanisms, and delivering the **technical specification** for the introduction of the IDC-ID. This will include, among other things:

- develop minimum standards and norms for the interoperability;
- attributing profiles for the minimum dataset (data formats) and associated metadata;
- presentation format (e.g., 2d barcodes, W3C verifiable credentials);
- level of assurance (as a reference point for interoperability);
- cryptography elements for data signing and encryption; and
- verification protocols for online and offline use cases.

Subsequently, a sample **implementation** (app or website) for basic verification of the IDC-ID can be developed by a group of AU Member States to test the interoperability of the credential and already support verifiable proofs of legal identity. The implementation will rely on the principle of privacy and security-by-design.

Participating entities will need to agree on the definition of **alternatives solutions to obtain an IDC-ID** for people that are currently excluded from any foundational ID system.

Additionally, a **mapping of other ongoing African Union initiatives** will be performed to build on the proposed framework (e.g., African Continental Qualifications Framework).

Phase 2 will then be concluded with the definition of a clear **action plan for the definition of the authentication infrastructure** as part of Phase 3.

4.3. DEVELOPMENT OF THE INFRASTRUCTURE TO ENABLE REMOTE AUTHENTICATION

Phase 3 will start implementing the Trust Framework defined as part of Phase 2.

In this phase, the layer that represents the issuance of the IDC-ID will be scaled up and expanded to implement an infrastructure that enables more advanced use cases such as remote authentication. This authentication layer will enable individuals to prove their identity digitally by exercising control of one or more authentication factors (e.g., a biometric or PIN code) bound to their previously verified legal identity, the IDC-ID.

Several technical options are available to AU Member States to implement this layer, including, for example, a federation of identity providers providing authentication mechanisms to the holders of the IDC-ID, or the development of digital ID wallet solutions or any other models enabling interoperability. Each of these implementations can offer a data minimisation option and selective disclosure services for specific use cases (for example by only sharing the relevant data points from an ID card and credit report to obtain a loan, seek social or health benefit, obtain a pension benefit), where authentication is legally required, or anonymising the IDC-ID minimum dataset (e.g., name, date of birth) into a proof of majority (+18y or +21y or a yes/no response).

AU Member States will also be able to seek further discussion and agreement on how to establish this authentication layer infrastructure and partner with RECs and other continental initiatives that are already investigating the introduction of digital ID interoperable solutions to access services remotely. Indeed, Member States and organisations will be able to leverage the standard-based common representation of identity information in a trusted and secure digital format and build additional services on top of it.

AU Member States will continue collaboration to strengthen the Trust Framework and governance and cooperation mechanisms following agreement on the additional infrastructures, following:

- **coordination with other initiatives** aiming at establishing interoperability at a continental level (e.g., SATA and RECs); and

- **agreement on the best architectural option** (e.g., federation, digital wallets, etc.) to develop the remote authentication function that would build on the IDC-ID.

Phase 3 will be concluded with a clear action plan on the implementation of the authentication layer, as per the architectural option to be agreed among AU Member States and organisations.

5. HIGH LEVEL ASSUMPTIONS, CHALLENGES AND RISKS

5.1. ASSUMPTIONS

Member States will adopt the framework, collaborate, commit to implement, and make necessary and required legal and regulatory reforms.

5.2. GENERAL CHALLENGES AND PROPOSED HIGH-LEVEL MITIGATIONS

The below table summarises the general challenges and proposed mitigation mechanisms.

#	Challenges	Proposed mitigations
1	Exclusion, weak security and erosion of personal data protection.	Apply the Principles defined in the framework (3.1) and strengthen the security and data protection legal frameworks and infrastructure in AU Member States.
2	Reluctance of AU Member States to adopt and implement the framework.	Raise awareness about benefits of interoperability framework at the domestic and continental levels and strengthen foundational ID systems.
3	Lack of technical and financial capability at AU Member States.	Enhance capacity and promote peer-to-peer knowledge exchanges among AU Member States, as well as consider cost effectiveness of technological solutions to be agreed on in Phases 2 and 3.
4	Inadequate data centres at the national/regional /continent levels.	Build national/regional/national data centres and promote their usage in Africa.

5.3. RISKS AND PROPOSED MITIGATIONS

The below table summarises the risks and proposed mitigation mechanisms:

#	Risks	Proposed Mitigations
1	Absence of proper definition of common standard and lack of understanding by AU Member States and failure to follow and adopt common standards.	Definition of standards and communication of same to AU Member States during implementation, and regular monitoring by a trusted and enabled Pan-African body that is supported and endorsed by all Member States of the same to ensure adherence to standards. Focused discussions and workshops with stakeholders to ensure clear definition of the standards for the chosen implementation strategy. Benchmarking the standard-based implementation strategy of AU Member States against similar, established standard-based national foundational ID programs across AU Member States.
2	Low levels of trust between national authorities with heterogeneous enforcement capacities lead to a slow uptake of the framework at a large continental scale. In addition, Member States' unwillingness to accept a supranational supervisory body, slow down the implementation of the Trust Framework.	The framework should target harmonisation and mutual recognition as a long-term objective but remain open for flexible and agile solutions to be developed, which could create shared audit mechanisms between willing countries to establish trust among themselves while remaining sovereign – through the unilateral recognition of issued trust certificates.
3	The solution, benefits, and options are not adapted well to the local environment or information is badly disseminated and the persons are not using the solution leading to poor uptake and ultimately high costs with little benefit.	Develop strong user-centric design structures to identify solutions that are easy to use and accessible to all. Develop strong dissemination mechanisms across AU Member States that incorporates all like-minded local actors.

#	Risks	Proposed Mitigations
4	Member States will decide on the appropriate technology during implementation phase, however if they opt for PKI technology, absence of continental level certifying institution and lack of inadequate governance the cryptographic requirements for the digital signature may prove to be a hindrance in the set-up of interoperability system.	Creation of a legal framework enabling the establishment of a continental level coordinating institution that is supported by an equitable governance structure accounting for the sovereignty of each Member State for implementation and management of digital signatures, its issuance, revocation and timely replacement and updating. Creation of a detailed and dynamic organisation structure to enable governance of digital signature/ PKI infrastructure across the implementation and the operations phase.
5	Due to incorrect and incomplete data, the design and implementation strategy of some of the interoperability components like digital signatures may be impacted. Delay in sharing of data and relevant information of the citizen or resident could also impact the timelines of the project.	Holding meetings with governments agencies for data gathering pertaining to implementation in the information gaps by leveraging the experience of the experts through peer-to-peer learning to encourage collaboration and regional and continental ownership. Monitoring of project timelines and milestones to prevent delays. It is also imperative to have a detailed and comprehensive implementation schedule which has been agreed upon by the AU Member States and key stakeholders.
6	Absence of clearly defined change management guidelines to ensure that the Framework remains aligned with current practices, needs, and technological development.	Putting in place a robust and well-defined change management process as part of the governance framework.
7	Member States will decide on the appropriate technology during implementation phase, however if they opt for PKI technology, certifying agencies in Africa may not reach a consensus regarding the management of PKI on the level of continent wide roll out. Secondly, there may not be consensus on setting up of digital signature exchange.	AU Member States either set up a new certifying institution for the management of PKI at the continent level or endorse a mechanism to bring the existing agencies on a common platform.
8	Not having the necessary minimum legal enabling environment in place at the national and regional level.	AU Member States to speed up the implementation of the required harmonised legal and regulatory frameworks.

6. ANNEX

6.1 WORKING DEFINITIONS

Attribute is a named quality or characteristic inherent in or ascribed to someone or something (adapted from NIST 800-63:2017). In ID systems, common identity attributes include name, age, sex, place of birth, address, fingerprints, photo, signature, identity number, etc.

Authentication is the process of establishing confidence that a person is who they claim to be. Digital authentication generally involves a person electronically presenting one or more "factors" to "assert" their identity—that is, to prove that they are the same person to whom the identity or credential was originally issued. These factors can include something a person knows (e.g., a password or PIN), has (e.g., an ID card, token, or mobile SIM card), or is (e.g., their fingerprints) (adapted from NIST 800-63:2017 and OWI 2017).

Authorisation is the process of determining what actions may be performed or services accessed on the basis of the asserted and authenticated identity (Nyst, et al. 2016).

Authoritative source of identity information is a repository or system that contains attributes about an individual and is considered to be the primary or most reliable source for this information. In the case that two or more systems have mismatched or have conflicting data, the data within the authoritative data source is considered the most accurate (FICAM, undated).

Claim is a qualification, achievement, quality, or piece of information about a subject's background such as a name, government ID, home address, or university degree (adapted from W3C).

Consent of the data subject means any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her.

Credential is a document, object, or data structure that vouches for the identity of a person through some method of trust and authentication. Common types of identity credentials include — but are not limited to — ID cards, certificates, numbers, passwords, or SIM cards. In the case of this Framework, the credential is a verifiable claim called IDC-ID.

Data controller means any natural or legal person, public or private, any other organisation or association which alone or jointly with others, decides to collect and process personal data and determines the purposes.

Data protection regulates how data is used or processed and by whom, and it ensures citizens have rights over their data. It is particularly important in ensuring digital dignity, as it can directly address the inherent power imbalance between 'data subjects' and the institutions or people who collected data.

Data protection authority (DPAs) is an independent public authority that monitors and supervises, through investigative and corrective powers, the application of the data protection law. They provide expert advice on data protection issues and handle complaints that may have breached the law.

Data sovereignty in this framework refers to personal data (including sensitive data) related to digital identification systems in an AU Member State must be collected, stored and processed (i) in facilities owned or controlled by and (ii) under the applicable law of the AU Member State.

Data subject means any natural person that is the subject of personal data processing.

Digital dignity (in the digital ID context) means that the human identity behind the digital ID has privacy and their data is protected.

Digital identification (ID) system is an identification system that uses digital technology throughout the identity lifecycle, including for data capture, validation, storage, and transfer; credential management; and identity verification and authentication (adapted from ID4D Public-Private Cooperation report).

Digital ID is a set of electronically captured and stored attributes and/or credentials that uniquely identify a person (adapted from Harbitz & Kentala 2013 and ID4D Technology Landscape report).

Digital signature is an asymmetric key operation where the private key is used to digitally sign data and the public key is used to verify the signature. Digital signatures provide authenticity protection, integrity protection, and non-repudiation, but not confidentiality protection (NIST 800-63:2017).

Digital stack, in the context of digital technologies, is a collection of independent software components or infrastructure that work together to support the execution of a use case.

Foundational ID system is an identification system primarily created to manage identity information for the general population and provide credentials that serve as proof of identity in order to access public and private services such as education, healthcare, social protection and financial services, etc. (adapted from Gelb & Clark 2013a and various ID4D publications). For the purposes of this Framework, AU Member States will decide which trusted data sources entail their foundational ID systems.

Functional ID system is an identification system created to manage identification, authentication, and authorisation for a particular service or transaction such as such as voting, tax administration, social programs and transfers, financial services, and more. Functional identity credentials — such as voter IDs, health and insurance records, tax ID numbers, ration cards, driver's licenses, etc. — may be commonly accepted as proof of identity for broader purposes outside of their original intent, particularly when there is no foundational ID system (adapted from Gelb & Clark 2013a and various ID4D publications).

Harmonisation is ensuring uniformity in the systems through the use of minimum standards to facilitate interoperability and legal and trust frameworks (e.g., for levels of assurance) to set rules and build confidence in respective systems.

ID is an acronym for identity credential or identity document in some areas.

Identification (ID) system is the databases, processes, technology, infrastructure, credentials, and legal frameworks associated with the capture, management, and use of personal identity data for a general or specific purpose (adapted from the Principles on Identification).

Identification is the process of establishing, determining, or recognizing a person's identity. (adapted from ISO/IEC 24760-1:2011 and ITU-T X.1252).

Identity is the relative social coordinates which distinguish one individual from another. Identity can change depending on the actors or the setting in which individuals find themselves and is therefore neither fixed nor absolute.

Identity provider is an authoritative entity — e.g., a government agency or private firm — that issues and manages legal identities, credentials, and authentication processes throughout the identity lifecycle (ID4D Public-Private Cooperation paper).

Interoperability is the ability of different function units – e.g., systems, databases, devices, or applications – to communicate, execute programs, or transfer data in a manner that requires the user to have little or no knowledge of those functional units (adapted from ISO/IEC 2382:2015).

Level of assurance (LOA) is the ability to determine, with some level of certainty or assurance, that a claim to a particular identity made by some person or entity can be trusted to actually be the claimant's "true" identity (ID4D Public-Private Cooperation). The overall level of assurance is a function of the degree of confidence that the applicant's claimed identity is their real identity (the identity assurance level or IAL), the strength of the authentication process (authentication assurance level or AAL), and—if using a federated identity—the assertion protocol used by the federation to communicate authentication and attribute information (federation assurance level or FAL) (adapted from NIST 800-63:2017).

Open standards are standards made available to the general public and are developed (or approved) and maintained via a collaborative and consensus driven process. "Open Standards" facilitate interoperability and data exchange among different products or services and are intended for widespread adoption (adopted from ITU-T).

Personal data means any information relating to an identified or identifiable natural person by which this person can be identified, directly or indirectly in particular by reference to an identification number or more factors specific to his/her physical, physiological, mental, economic, cultural or social identity.

Privacy- and security-by-design means proactively embedding privacy and security mechanisms into the design and operation of products and services both non-IT and IT systems, networked infrastructure, and business practices. This requires that privacy and security governance is considered throughout the whole engineering process and product lifecycle.

Data Protection Impact Assessment (DPIA) is a process designed to identify risks arising out of the processing of personal data and to minimise these risks as far and as early as possible. DPIAs are important tools for negating risk, and for demonstrating compliance with the data protection laws and regulations.

Processing of personal data means any operation or set of operations which is performed upon personal data, whether or not by automatic means such as the collection, recording, organisation, storage, adaptation, alteration, retrieval, backup, copy, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination and locking, encryption, erasure or destruction of personal data.

Proof of legal identity is a credential, such as a birth certificate, identity card or digital ID credential, that is recognised as proof of legal identity under national law and in accordance with emerging international norms and principles (United Nations Legal Identity Expert Group Operational Definition of Legal Identity).

Relying party (RP) is an entity that relies upon the credentials and authentication mechanisms provided by an ID system, typically to process a transaction or grant access to information or a to system (adapted from NIST 800-63:2017).

Trust Framework refers to business, technical, operational, and legal requirements for the identity system to foster interoperability between the various participating parties.

Verifiable presentation is a tamper-evident presentation (data derived from one or more verifiable credentials) encoded in such a way that authorship of the data can be trusted after a process of cryptographic verification, e.g., selective disclosure approaches that synthesize data and do not transmit the original verifiable credentials (definition adapted from W3C).

Verification is defined as the process of verifying specific identity attributes or determining the authenticity of credentials in order to facilitate authorisation for a particular service.

African Union

Bureau of the Chairperson
African Union Headquaters
P.O. Box 3243, Roosevelt Street
W21K19, Addis Ababa, Ethiopia
Tel: +251 (0) 11 551 77 00
Fax: +251 (0) 11 551 78 44
www.au.int