UNIVERSITY OF NAIROBI

COLLEGE OF BIOLOGICAL AND PHYSICAL SCIENCES

ENHANCED DIGITAL IDENTITY MODEL FOR HUMANITARIAN AGENCIES IN KENYA

BY

JOHN MAGAIWA MENG'ANYI
P54/85695/2016

SUPERVISOR:
DR. SAMUEL N. RUHIU

AUGUST 2022

A project report submitted in partial fulfillment of the requirements for the award of Master of Science in Information Technology Management of the University of Nairobi

DECLARATION

I declare that this project report is my original work except where due references are cited. To the best of my knowledge, it has not been submitted for any other award in any university.

John — 30/8/2022

John Magaiwa Meng'anyi — Date

Reg No.: P54/85695/2016

This project report has been submitted in partial fulfillment of the requirement of the Masters of Science Degree in Information Technology Management of the University of Nairobi with my approval as the University Supervisor.

1/Sep/22

Samuel N. Ruhiu — Date

University Supervisor

ACKNOWLEDGEMENT

I am grateful to God for the ability, favor and blessings that that he has granted me through this journey to completion.

My sincere appreciation to my supervisor, Dr. Samuel Ruhiu for his support, positive criticism, and overall contribution towards my project work.

Finally I thank my mum and family, for all the support and constant follow-up throughout the project period.

ABSTRACT

Digital identity systems have the ability to enhance the core elements of the sustainable development goals ensuring no one is left behind. These includes, enhancing digital inclusion, strengthening access to legal identity, improved accountability and effectiveness in delivery of social protection.

Humanitarian agencies are exposed to risks such as commodity losses, disallowed costs, and damaged reputation caused by shortfalls in the existing beneficiary identification systems that have led to falsification of identity documents, siloed registries, duplication of assistance, and inadequate privacy safeguards. The study aimed to develop an enhanced digital identity model for beneficiary targetting and registration that will support equal access to data for all humanitarian actors and linkages with civil registries. The literature review details the Kenyan identity eco-system and discusses identity frameworks within the humanitarian sector.

The study further discusses factors affecting beneficiary identification and the current digital identity trends in social protection. The proposed conceptual model was adopted from the Christopher Allen Self Sovereign identity framework and the World Bank identity guidelines. A survey was conducted to obtain quantitative data from 74 humanitarian actors, and the sample data was evaluated using factor and regression analysis. The study found that access, privacy, persistence, governance, and interoperability are the key components when designing a beneficiary-centric identity system for humanitarian actors. Awareness, funding, resource allocation, support and ownership were moderating, affecting all the relationships between the independent and dependent variables.

TABLE OF CONTENT

TABLE OF FIGURES

TABLE OF TABLES

CHAPTER ONE: INTRODUCTION

1.1 Background of Study

Legal identity is a vital element of human rights and development. The Bill of Rights in the Constitution of Kenya, 2010, secures freedom for it's citizens to move around, live where they choose, and have rights in their socioeconomic lives. However, Kenyan citizens' rights, privileges, and benefits are subject to obtaining registration and identification documents.

According to the United Nations Convention on the Rights of the Child, every child has the right to a name and to have that name recorded at the time of birth. Birth registration is the initial step within a sturdy civil registry system. Whereas the Civil Registration Service Charter stipulates instant issuance of birth certificates, it takes more than a month to acquire this vital document (CAJ, 2015). Births that occur in institutions, such as hospitals, are well documented. However, those happening outside the established facilities are not recorded, making it hard for the parents to obtain birth certificates. A birth certificate is a requirement when applying for a National Identity (ID) card for persons without a parents ID. It is also mandatory for passport application and registration of candidates for the National examinations through the National Education Management Information System (NEMIS).

Approximately 1.1 billion individuals globally are denied access to essential services and rights because they lack legal identity and remain invisible(USAID, 2018). Most Kenyans, especially those residing in Arid and Semi-Arid Lands (ASAL) and informal urban settlements, do not understand the need to prepare for the eventuality of needing to provide a valid form of identification (CAJ, 2015). According to the CAJ report, it takes 2-4 months to obtain an ID card and travel an average of 25kms to access this service. Communities living near the borders of Kenya have to undergo an extra level of verification even where they have proof of being Kenyans.

The Shona, The Pemba, Congolese, and Rwandans are among the stateless communities who have lived in Kenya going up to the fourth generation. These communities cannot prove their origin or obtain identification documents since they do not have a legal identity. The community members are exposed to exploitation by intermediaries when seeking to obtain fundamental rights and services. They cannot enjoy economic rights to employment and ownership of property or

business. These stateless persons do not enjoy the right to move freely within and outside the country, and their children cannot access identity documents to enable them to register for National examinations. The community's women cannot access government-subsidized medical care, especially pregnant and nursing mothers.

The political process in Kenya significantly affects the demand for identification documents occasioning spikes in the number of applications for IDs during the electioneering period and increased political mistrust over voter registration. During the 2017 General Elections, public authorities mismanaged and even disclosed voters' sensitive information to political candidates (Muthuri, 2018). The communications sent to respondents had information identifying the respondent's name or voting area, demonstrating that political candidates could collect data sets of voters they want to target directly.

Community members with a national ID must bring it for ease of identification and registration during emergencies though holding a national ID is not a prerequisite for receiving assistance(WFP, 2015). Beneficiary identification systems in the Humanitarian sector experience similar challenges to civil registries and therefore need linkages to strengthen their capabilities. Lack of connections to civil registries, which are the sources of truth, exposes humanitarian actors to the risk of cash transfers to terrorists for communities living along the borders or working within affected areas.

Individuals engaging in manual work for income-generating activities denature their fingerprints, making it difficult to pick them up by manual or digital registration forms (Schoemakert, 2019). Their applications are declined and required to grow back their fingerprints which takes up to a year of not doing any manual task, thus denying them a source of income. These individuals will continue their daily lives without legal identification documents due to a lack of alternative means to capture their biometrics.

The data currently hosted in the Social protection Single Registry only covers a tiny part of the nation's frail population and lacks critical datasets such as vulnerability types, location data, phone numbers, coping strategies, and geo-data (Gardner, 2020). Furthermore, there are challenges with data quality, such as wrong names and identification details. Also, access to the data was viewed to be bureaucratic and time-consuming.

Humanitarian organizations still use paper-based methods or flat-file databases such as excel sheets or relational databases to store and administer beneficiary records. The tools currently in use are not tamper-proof and do not have adequate security and privacy safeguards. Access by unauthorized persons could lead to falsification of records and cash transfers going to the wrong individuals.

1.2 Problem Statement

A government-issued identifier is a requirement before an individual can benefit from formal employment, register for a SIM card, open a bank account, or access government and business offices. A national ID card is not a requirement for receiving humanitarian assistance such as in-kind distributions, Non-food items, or vouchers though it eases the identification process. It is mandatory to have a National ID to open a bank account or register SIM card before benefiting from cash assistance interventions.

The social protection single registry aggregates data from the main social protection safety nets and links to the Integrated Population Registration System (IPRS) for ID verification. The registry has beneficiary data of the four main cash transfer projects, excluding several other in-kind, Non-food items, and voucher interventions implemented in Kenya. Access to the Single registry is a bureaucratic process and limited to a few humanitarian actors (Gardner, 2020). Further, the data quality in the registry is unreliable for emergency responses because of missing data sets, data errors, inconsistent sync from source management information systems, and excludes most vulnerable households.

The beneficiary profile includes information on vulnerabilities, GPS location, household member details, bank account details, mobile phone numbers, and biometrics. This information is not available within government civil registries or an integrated platform that consolidates all this information from multiple sources and provides humanitarian agencies access to the information. Because of specific data requirements, humanitarian agencies develop functional identity management systems to collect qualitative and quantitative beneficiary data to deliver life-saving assistance.

The fallible and disjointed beneficiary identification systems among humanitarian actors have resulted in identity sprawl, duplication of efforts, and expensive registration processes within the humanitarian sector. People who receive benefits do not have the ability or authority to control their digital identity.

1.3. Overall Objective

This research aims to develop an enhanced digital identity model for beneficiary targeting and registration. The proposed model will support equal access to data for all humanitarian actors and linkages with civil registries.

Specific Objectives

1. Analyze identity trends in Kenya
2. Identify the factors affecting identity systems in the humanitarian sector in Kenya
3. Identify what is needed for establishing an identity system for the humanitarian sector.
4. Propose an enhanced digital identity model for beneficiary targeting and registration for Humanitarian actors in the country

1.4. Research Questions

1. What are the current identity trends in Kenya?
2. What are the drivers and barriers of digital identity within the humanitarian sector in Kenya?
3. What are the components of an identity system for the humanitarian sector?
4. What are the primary essentials of a multiagency digital identity model for beneficiaries of humanitarian responses in the country?

1.5. Scope of the Research

The study was conducted among eight humanitarian Agencies that are first responders during emergencies, two County Governments, and The Ministry of Labour and Social protection. Project Managers, Program officers, volunteers, field officers, and frontline staff responded to questionnaires.

1.6. Significance of the Research

The study outcomes will contribute to understanding identity trends in the social protection sector and Kenya. The study will improve digital identity knowledge by identifying the humanitarian sector's drivers and barriers. Humanitarian actors will benefit from cost savings associated with beneficiary registration, better coordination, and data sharing mechanisms. Beneficiaries will be served better and promptly once the proposed model is implemented.

CHAPTER TWO: LITERATURE REVIEW

2.1. Introduction

The literature review section examines existing research on identity sourced from journal articles, research papers, and content published on the internet. This section is organized into the discussion on Identity types, the Kenya identity ecosystem, digital identity using blockchain technology, a review of digital identity models, and a proposed conceptual model.

2.2. Identity

According to ISO/IEC 24760-1, identity is a set of attributes relating to an entity. It further states that an entity can have more than one identity, and several entities can have the same identity. More characteristics mean a more robust identity (Alemayehu & Mwangi, 2011). That is correct, even if the characters in question are unique. Individual communities will develop their systems of mutual identification. As a result, no silver bullet will work for everyone (Alsayed Kassem et al., 2019).

An attribute is a specific characteristic related to an individual or a thing. Attributes can be temporary or permanent. For example, biometric data, Date of Birth (DoB), and Government issued Identification Documents (IDs).

2.2.1. Legislation on Identity

Target 16.9 of the Sustainable Development Goals (SDGs) is to ensure that everyone has a form of legal identification by the year 2030. Freedom of movement, freedom of residence choice, and freedom to dwell in any country are also guaranteed under Article 12 of the International Covenant on Civil and Political Rights.

The Constitution of Kenya 2010 allows citizenship to be granted upon birth, marriage, or long-term residency. Dual citizenship is recognized by the constitution. The Ministry of Interior issues identification documents to citizens using laws such as the Registration of Persons Act (1949), Births and Deaths Registration Act (1928), Kenya Citizenship and Immigration Act (2011), and Refugees Act (2006).

The National Hospital Insurance Fund Act (1998) and the National Social Security Fund Act (2013) govern the issuance and use of functional IDs that target specific services. The Kenya Citizens and Foreign Nationals Management Service Act (2011) enables Integrated Population Registration System IPRS. Section 9A of the Registration Act (1949), which establishes the National Integrated Identity Management System (Huduma Number) is also a part of the Integrated Population Registration System.

2.2.2 Self Sovereign Identity

The Self Sovereign Identification (Zheng and al., 2017) is an identity management mechanism where individuals own and control their digital identities. The Self Sovereign identity is portable, secure, and private.

Three actors make up Self Sovereign Identity. They are the claim-issuer (user) and the relying person (Muhle et al., 2018). The claim-issuer issues an identity which attests to specific attributes about the user. The user controls this identity. The user's identity will be provided to a relying party for identification purposes. The relying person must trust the claim issuer to accept the identity. Below is a diagram that shows the relationship between the various actors in the SSI system.

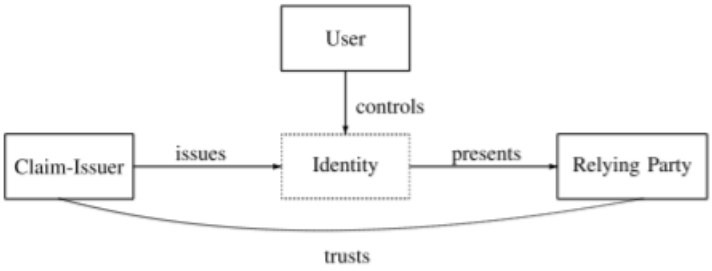

Figure 1: Self-soverign identity actors

The Self-sovereign Identity model eliminates third-party Identity providers and allows for direct connectivity between users and organizations. Digital wallets save all identity-related confidential and personal data, giving the user full ownership and control.

2.3. Kenya Identity Ecosystem

The Government or mobile network operators are the primary issuers of identification credentials in Kenya (Schoemakert, 2019). Government-issued identifiers include an identity card (ID), passport, birth and death certificate. Additional identifiers issued by other government agencies include National Hospital Insurance Fund (NHIF) number, National Social Security Fund (NSSF) number, voter cards, KRA PIN, and driver's license. Financial and mobile service providers also issue identifiers such as Bank Account Numbers, Mobile phone numbers, and digital credit profiles. Likewise, development partners assign IDs to beneficiaries for verification purposes when delivering assistance.

The Kenyan Government has been keeping records of its citizens since 1915, when the colonial Government issued 'kipande' to control male Africans into colonial labor. In 1947, a passbook was mandatory for all males above sixteen to distinguish between the protectorate and non-protectorate persons. In 1980 the legislation on identity was amended to allow women to be registered and introduce the 1st generation identity cards. The 2nd generation laminated cards introduced in 1995 were smaller in size, laminated, and had basic information such as name, gender, photo, geographical origin, release date, and image of one fingerprint. It also has an eight-digit ID number and a nine-digit serial number.

In 2011, the GoK introduced plastic cards to replace the damage-prone 2nd generation cards. In 2019, The Government started the roll-out of the Huduma number, a number granted to each citizen at birth or enrollment that remains with them until they relocate outside Kenya or death. A chip-based huduma card is issued to all registered persons to facilitate access to government services and essentially act as a passport inside the East African Community.

2.3.1 Integrated Population Registration System (IPRS)

Vision 2030's flagship project is the Integrated Population Registration System (IPRS). It is envisioned to be a national population register and a single source of truth about the identities of all Kenyans and foreign residents. (Gok, 2018). The system is expected to generate and assign unique integrated personal numbers and establish a framework for sharing information and population data with Government and private bodies. Lack of transparency and a proper legal

framework raises concerns about how sensitive data is managed and what consequences it could have for consumers.

The automatic two-way links between credit reference bureaus and IPRS provide a quick, efficient, and real-time sorting system for mobile credit providers in search for on the spot decision-making (Schoemakert, 2019).

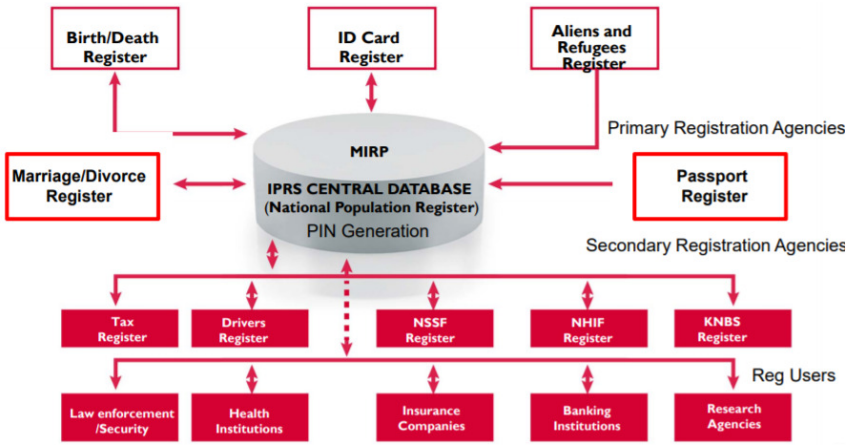

Figure 2: Kenya Integrated Population Registration System (Schoemakert, 2019)

2.3.2. National Integrated Identity Management System (NIIMS)

The National Integrated Identity Management System (NIIMS) or Huduma Namba, aims to develop and maintain a central repository of data on all persons residing in Kenya (GoK, 2021). The Huduma Namba will improve service delivery in the country by harmonizing and standardizing residents' data, allowing for more accurate resource planning and allocation.

The rollout of the Huduma Namba is marred by legal suits challenging the ability of the Government to ensure adequate data privacy and security safeguards for the collection and administration of sensitive data, the inability to resolve discriminatory treatment and lack of identification of marginalized groups. There are many similarities in the functions of the IPRS and NIIMS since both generate unique identifiers and link to civil registries and other government functional databases such as NSSF, NHIF, and KRA.

Other countries that have adopted multipurpose digital identity schemes include India, Estonia, and Nigeria. India's adhaar has been linked with various services, including delivering subsidies that successfully eliminated "ghost beneficiaries." It provides multiple options for authentication, such as face recognition, iris scan, ten fingerprints, and one-time password (OTP). Estonia provides a secure digital residency regardless of whether they live within the country. A smart chip-based ID card is issued to successful applicants, which grants digital identification and authorization to make secure transactions and digitally sign documents.

2.3.3 Social Protection Single Registry

The single registry consolidates information from all social protection schemes. It provides a single platform on which common and essential information across social security programs can be stored, analyzed, and reported for the benefit of stakeholders. The single registry helps eliminate fraud by verifying beneficiary details against the National Population Registry (IPRS). It also allows checks to verify if a beneficiary receives multiple benefits within the program.

The single registry stores data from social protection interventions such as the National Safety Net Programme, the Older Persons Cash Transfer (OP-CT), the Persons with Severe Disabilities cash Transfer (PWSDCT), the Hunger Safety Net Programme (HSNP), and Cash Transfer for Orphans and Vulnerable Children (CT-OVC). The Single Registry's current data sources are shown in Figure 3.

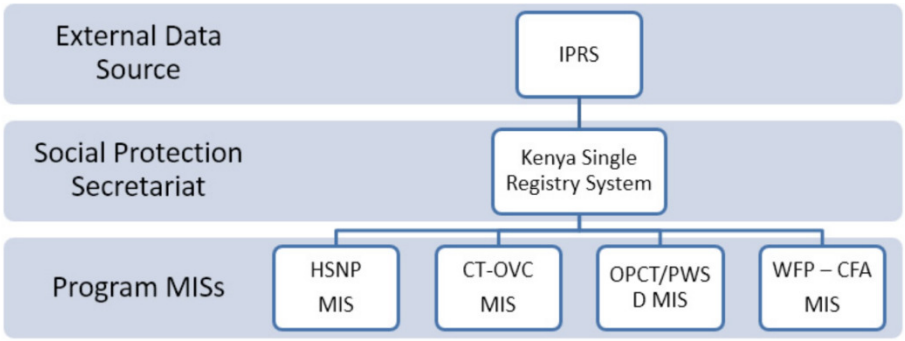

Figure 3:Social protection Single Registry Data Sources

2.3.4 Digital Credit

After an automated eligibility screening process, digital-based microcredit allows users to borrow small amounts from financial institutions immediately. Digital credit is an 'in-facto' form of identification that relies on individuals' credit ratings (ITU-T, 2017). It can be accessed using several data points such as government issued credentials and mobile phone and social network usage patterns. These data points are combined with customer borrowing and repayment history to estimate providers' risk in loaning them (Schoemakert, 2019). Credit scores are stored by credit rating companies or shared with other agencies for a fee.

Privacy, data protection, and exclusion of vulnerable groups are some of the concerns arising from introduction of digital credit. Consumers enroll for digital credit without reading the terms and conditions thus subjecting them to unlimited SMS notifications, full disclosure of their data to third parties, and a waiver on their right to dignity (Muthuri, 2018).

2.4. Digital Identity

Digital identity refers to the online persona of a subject. (Grassi and al., 2017). The International Telecommunication Union (ITU) defines digital identity as the digital representation of an entity that is detailed enough to distinguish the individual within the digital context. The world bank defines identity as the building blocks that include storing identity data and granting identity credentials.

The information that makes up an individual's digital identity can easily be divided into two broad categories: digital attributes and digital actions (Domingo and Enriquez, 2018). Digital attributes include login credentials (username and passwords), bank details, email address, and biometrics. Digital actions consist of comments, likes, and shares on social media sites, purchase history and forum posts, geotagging and downloaded Apps.

Digital identity has evolved through three phases(Naik & Jenkins, 2020). Digital Identity 1.0 enabled logging into websites using credentials such as usernames and passwords. Digital Identity 2.0 advanced logging into websites by allowing users to use their existing social account credentials. Currently, we are in the age of next-generation Digital Identity 3.0, where consumers' real identities are intertwined with their virtual lives. It is accompanied by new and secure

protocols, enhanced authentication mechanisms like biometrics, and innovative real-time applications, including online banks and e-wallets. Digital identity has introduced concepts such as;

2.4.1. Digital Identity proofing

Identity proofing refers to verifying the legal identity of the entity that presents themselves for registration (ITU-T, 2017). A digital identification is issued and linked to a person once the identity proofing phase is completed. The first step to establishing trust and security is digital identity verification (USAID, 2018).

2.4.2 Identity Authentication

Authentication is the process of validating the assertion of an attribute associated with an identity established during identification proofing phase(ITU-T. X.1252, 2010). This involves associating an identifier with the individual or device.

ITUX.1254 defines four elements as the cornerstones for authentication: something an entity has; something an entity knows, something an entity is, and something that an entity does most often. The number of factors included in an authentication system determines its strength (Grassi & co., 2017).

Digital authentication can be use for passwords, biometrics, knowledge-based questions, and one-time passwords. It also includes document authentication, mobile authentication, third-party authentication, and authentication apps. To enable web-based authentication and authorization, protocols such as OAUTH2, SAML, OpenID, and SAML are used.

2.4.3 Identity Assurance

Identity assurance (or confidence) refers to the level of certainty that an identity you are interacting with is genuine and belongs to the person using it (ITU-T, 2017). Digital identity assurance is essential for online trust, security, and access control. There are three types of assurance to establish trust in a digital ID: authentication assurance, identity assurance, and federation assurance. The identity verification process is called Identity Assurance Level (IAL), Authentication Assurance Layer (AAL) refers to the authentication process while Federation

Assurance Level is the assertion protocol federated environments to communicate attribute and authentication information to relying parties.

2.4.4 Authorization

Authorization is deciding how much of a service a user can access after verifying their identification (Grassi et al., 2017). Control over resources requires verifying the identity first(ITU-T X.1254, 2021). The figure below shows the high-level digital identity process flow.

Figure 4: High level Digital Identity process flow

2.4.5. Digital Identity Management

An identity Management System is a system that manages identity information through registering, revoking, updating, and looking up digital identities (ITU-TX.1254,2021).

A multi-layered approach has been used in the development of digital identity systems. The standards that govern system operation are at the bottom while the top is service delivery.

Table 1: Digital Identity System Categories

Category	**Description**
Internal identity management	One entity can be both the identity provider as well as the relying agent.
External authentication	Multiple identity providers authenticate users to one relying party

Centralized identity	Many identity providers offer many different services to different relying parties
Federated identity	One entity can be both the identity provider as well as the relying agent.
Distributed identity	Multiple identity providers authenticate users to one relying party

Identity management systems can further be characterized by either purpose or design. ID systems with a functional purpose tend to be instrumental by design while foundational systems are infrastructural by design(USAID, 2018).

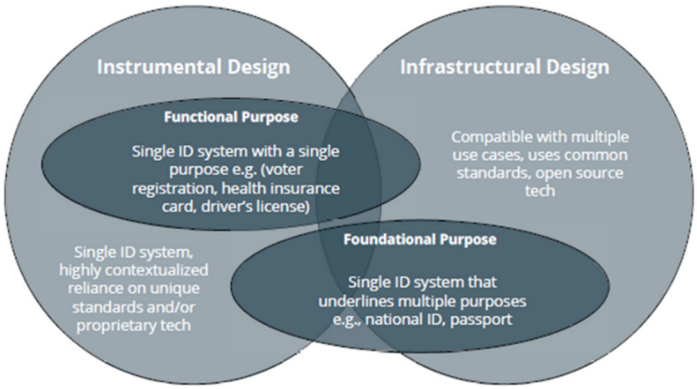

Figure 5: Categories of Identification Systems (USAID, 2018)

2.5. Beneficiary Targetting and Registration

Beneficiary registration is the systematic collection of data about a particular individual or a group to identify and understand their characteristics with an intention to protect their rights and meet their needs during crisis through recovery and transition phases.

Beneficiary targeting and registration exercise is a resource-intensive and time-consuming process requiring proper planning. Careful preparation and planning for each step:

- The identification of the population to be registered and involved actors (national authorities, NGOs, site management authority).
- The registration itself.
- Data encoding, verification, quality control, analysis, and dissemination.
- Updates based on the evolving situation.

In most contexts, a beneficiary is only eligible to benefit from a humanitarian program if registered. Beneficiary targeting uses self-selection, community-based selection, vulnerability assessments, and geographical targeting. The following steps are required to write a beneficiary for a trusted digital identity:

1. Capture attributes for biographic and/or biometric data
2. Use biometrics or other third-party checks to verify the authenticity of the documents and confirm the identity of the person who presented them
3. These digital IDs can finally be digitized

Competition, data security and privacy concerns have inhibited data sharing among humanitarian actors even when operating in the same locality and reaching the same beneficiaries. Advanced technologies such as blockchain provide capabilities to address identity challenges within the humanitarian sector.

2.6 . Blockchain

Blockchains are tamperproof and tamper-resistant digital ledgers that are distributed and often without a central authority(Dylan Yaga, 2018). Blockchain is applied in identity management to act as a single source of truth for network members about valid credentials and who attested that the credential was valid (Stokkink, Pouwelse 2018). The verifier's judgment of the reliability and validity of the attestor is what validates proof.

The permission model of blockchain networks determines who can manage them (Alsayed Kassem & co., 2019). Permissionless blockchain networks allow anyone to publish blocks on decentralized ledger platforms without requiring permission from any authority. Blockchain's main components

are cryptographic hash functions and transactions. They also include addresses, ledgers, block information, and how blocks are linked together (Dylan Yaga 2018, 2018).

2.6.1. Hashing

The term "hashing" refers to the use of a cryptographic "hash function" on data. For inputs of virtually any size, this will calculate a distinct output. Blockchain technology employs a wide variety of cryptographic hash algorithms, such as SHA-256 and Keccak. Among the many uses for cryptographic hash functions include preventing address derivation, generating unique identifiers, encrypting block contents, and safeguarding the block header (Slavin, 2019).

2.6.2. Asymmetric Key Cryptography

Asymmetric key cryptography uses a public and private key to encrypt data. These keys are mathematically related (Zheng et al., 2017). While the public key can be made public to increase security, the private key must remain confidential if data is protected by cryptographic protection. Transactions can only be decrypted with the public key. Alternately, access to data encrypted with the user's private key is limited to those who can decrypt it.

2.6.3 Ledgers

A ledger is a record of transactions. This is possible with blockchain technology, which combines distributed ownership and a distributed physical structure (Slavin, 2019). Blockchain networks' distributed physical architecture often uses more computers than the centrally managed physical infrastructure. Distributed ownership of ledgers is growing in popularity due to the trust, security, and reliability issues associated with ledgers with central ownership.

2.6.4 Blocks

Publishing nodes add new transactions to the distributed ledger each time they publish a block. To ensure that all transactions in a published block are legitimate, other full nodes will do their own validations before accepting the block. Any changes to blocks previously published require a different hash. As the previous block's hash is included, amendments would be made to the hashes of any subsequent blocks. This allows for easy detection and rejection of altered blocks. Below is a generic blockchain.

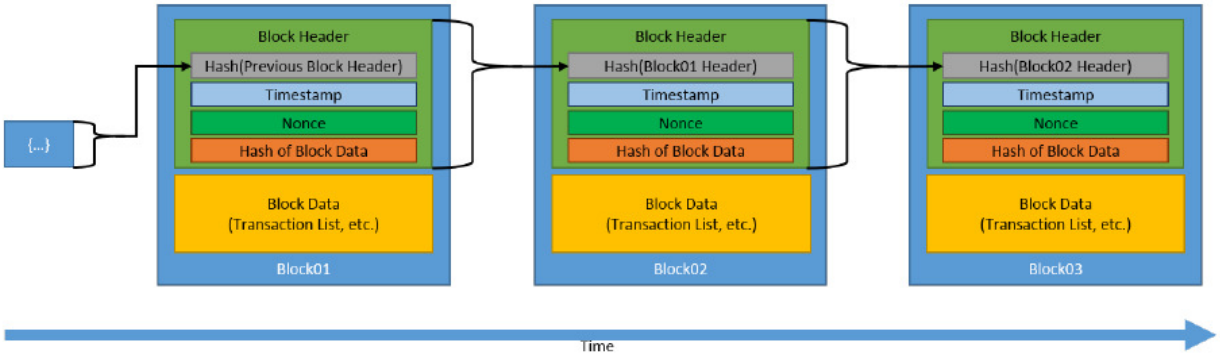

Figure 6: Generic Chain of blocks

2.7. Case Studies Beneficiary Information Management Systems

Beneficiary Information Management Systems seek to strengthen efficiency, effectiveness, and accountability in delivering humanitarian interventions to the vulnerable people. The system functions include digital identities, intervention setup, distribution planning, transfers, attendance tracking, and reporting. These functions are supported by a combination of offline and online tools on digital devices.

Each registered beneficiary is assigned a digital ID for authentication and data exchange. Biometrics functionality is used for deduplicating and authentication during assistance delivery. Distributed items include cash, vouchers, food and non-food items.

Access to the system is password-authenticated and role-based. These systems are bespoke or offered as Software as a Service by private agencies. Most systems have incorporated data security and privacy safeguards such as data residency, data encryption, established data retention and protection policies, data sharing agreements, and routine third-party audit checks. Most information systems lack a complaints response mechanism to handle feedback from the beneficiaries. Also, they are not linked to civil registries, thus the identifier is limited to the project life-cycle.

World Vision's Last Mile Mobile Solution (LMMS), WFP's SCOPE, UNHCR's BIMS, ONE platform, and COMPAS are the established information systems in the humanitarian sector in Kenya.

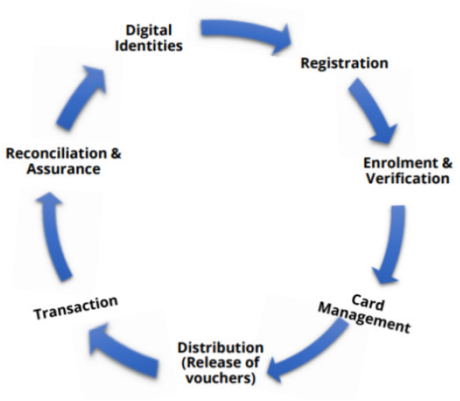

Figure 7: WFP Beneficiary information and transfer management cycle

2.8. Theoretical Models

The research reviewed digital identity guidelines and models to understand the critical components of a digital identification system. The model and guidelines apply to address the core objective of the research, which is to develop an enhanced digital identity model for beneficiary targeting and registration for the humanitarian sector in Kenya. The following section provides a detailed analysis of the guidelines and models.

2.8.1 Identification principles for sustainable development (World Bank Group, 2021)

The World Bank (2021) outlines ten principles centered on the themes of design inclusion and governance to help guide the application of identity programs for sustainable development. The principles are applicable to both manual and digital foundational identification systems. They are broad to accommodate identification systems by different providers, technology, architecture, function, and governance arrangements. The table below outlines the ten principles.

Table 2: World Bank Principles on identification for sustainable development

Theme	**Principle**
Inclusion	All individuals are covered from birth through death without discrimination
	Eliminate barriers that hinder access to information and technology.

Design	Create a robust, inimitable, secure, and accurate identity
	Create a tool that responds to users' needs and is interoperable
	Vendor and technology neutrality are key to ensuring open standards
	Use system design to control and protect user privacy
	Considering uncompromised accessibility, plan for sustainable financial operations
Governance	Use a comprehensive legal framework it will help you protect your data privacy and user rights.
	Clear institutional mandates and accountability should be established
	Through independent oversight and adjudication of grievances, enforce legal and trust frameworks

2.8.2 NIST Digital Identity Model(Grassi et al., 2017)

The NIST digital identification model describes the interactions among actors in a digital identity system. Through an enrollment process, an applicant submits an application to become a subscriber through a Credential Service Provider (CSP). The CSP performs verification checks on the applicant's identity before enrolling them as a subscriber. The CSP and subscriber establish an authenticator and a corresponding credential. CSP keeps the credential, its status, and all enrollment data for the life of the credential. The subscriber keeps their authenticator(s).

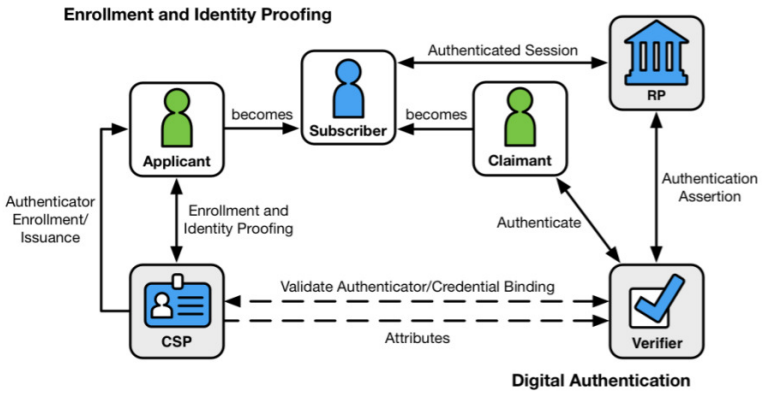

Figure 8: NIST Digital Identity Model (Grassi et al., 2017)

2.8.3 Unified digital ID framework (Geteloma et al., 2019)

The three tiered unified digital ID framework is based on the German eCard plan. The application layer allows the framework to be communicated via a client's web browser. The Identity layer is in charge of the electronic card interface and the management interface. The Authentication layer supports technologies such as NFC smart cards,biometrics and one-time passwords.

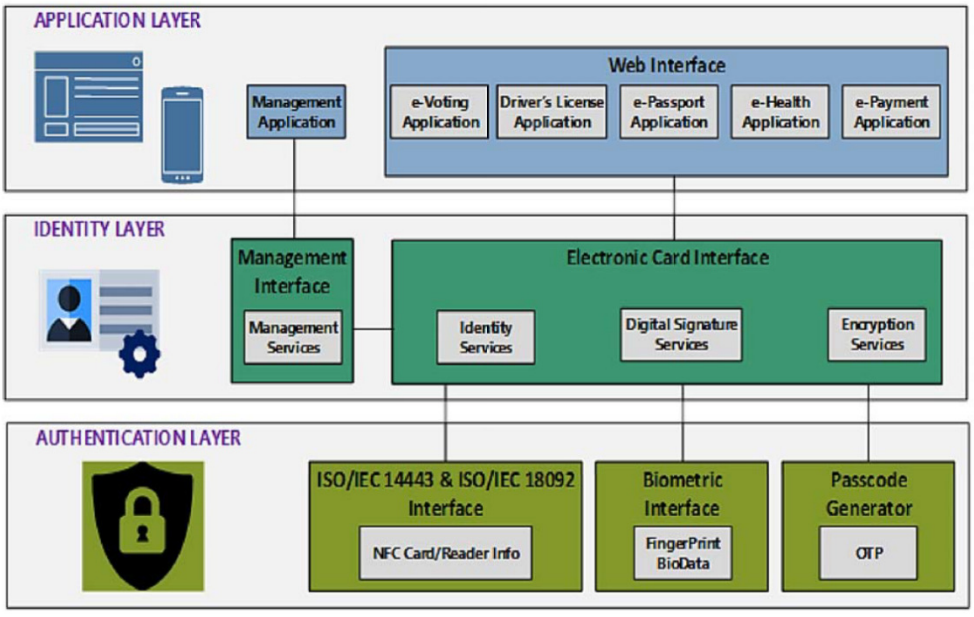

Figure 9: Unified Digital ID framework (Geteloma et al., 2019)

2.8.4 C.Allen ten properties of Self Sovereign Identity(Allen, 2016)

C.Allen's properties on self sovereign identity draws insights from Cameron's Laws of Identity and The World Wide Web Consortium (W3C) Verifiable Claims Task Force. These ten principles not only guarantee user control, but also support transparency and fairness. The ten properties are analysed in the table below

Table 3: C. Allen 10 properties of Self-Sovereign Identity

Principle	**Description**
Existence	Users need to be able to live independently.
Control	Users need to control their identities.
Access	Access to data must be granted to users.
Transparency	Transparency is essential for algorithms and systems.
Persistence	Identities should be kept alive.
Portability	Information and services regarding identity must be easily transportable
Interoperability	Identities should always be widely accessible.
Consent	All users must consent to the use of their identity.
Minimalization	Limit disclosure of claims.
Protection	Users' rights must be protected

2.8.5 Digital Identity Life Cycle

Digital identity lifecycle has three fundamental stages: (a) registration (b) The issuance of credentials (c) authentication to service delivery . Registration is a two-step process starting with enrollment where key identity attributes are captured followed by identity validation to ensure the person exists and only one person claims the identity. Validation can be through physical

validation of documents, deduplication process or linkages with other databases. Credentials such as smart cards, barcode card and mobile identity are issued to validated individuals enabling them access to associated benefits and services. The Figure below illustrates digital identity life cycle of the online identity model

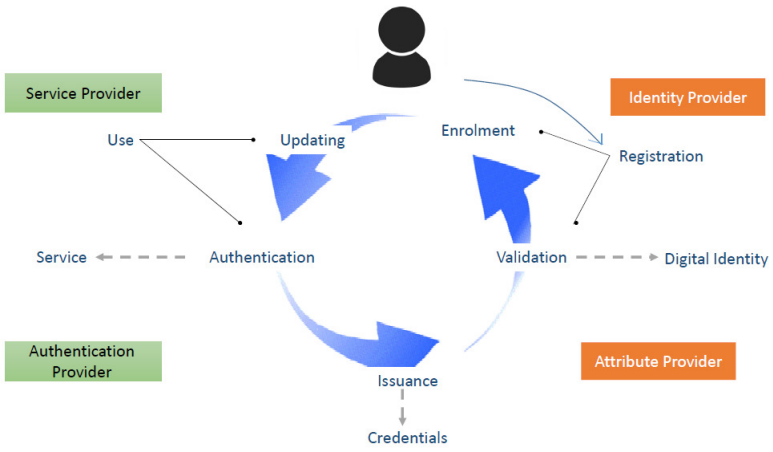

Figure 10: Digital Identity Life cycle

2.8.6 Summary of theoretical models

The research analysed four digital identity frameworks which are applicable for the study. The frameworks outline key components of identification systems. Further, the architecture has enhanced security and privacy features.

Table 4: Summary of Theoretical Models

Model	Summary
World Banks Identity Framework (World Bank Group, 2021)	Lists 10 principles for identification in sustainable development . The identification principles are focused on creation and use of legal and functional identification systems. The principles are developed by development partners but haven't been supported by a greater number of stakeholders including gorvernments.
NIST Digital Identity Model (Grassi et al., 2017)	The digital identity model represents the architectures that are currently on the market. These guidelines are limited to the authentication and identity proofing of users who interact with IT systems over a network.

Unified Digital Identity Framework (Geteloma et al., 2019)	The framework seeks to mitigate against the multiplicity of identification systems. Application Layer, Identity Layer, and Authentication Layer make up the three tiers of the framework. The framework concentrates on specification of homogeneous interfaces for a standardized usage of different eCards in various applications
Christopher Allen Identity Framework (Allen, 2016)	The model provides a summary of ten principles of identity with focus on self-sovreign identity. The principles are focused on the user, their rights and the infrastructure on which identity systems are based. This model allows users to control their digital identities and not rely on service providers to manage their data.

2.9. Conceptual Model

The study seeks to identify the main components of an identity system for the humanitarian sector. The proposed conceptual model was adopted from the Christopher Allen's Identity framework and the World Bank identity guidelines. These two frameworks provide the core components to develop and implement a beneficiary-centric identity system. Further, they ensure identity systems are inclusive, accountable, and trusted.

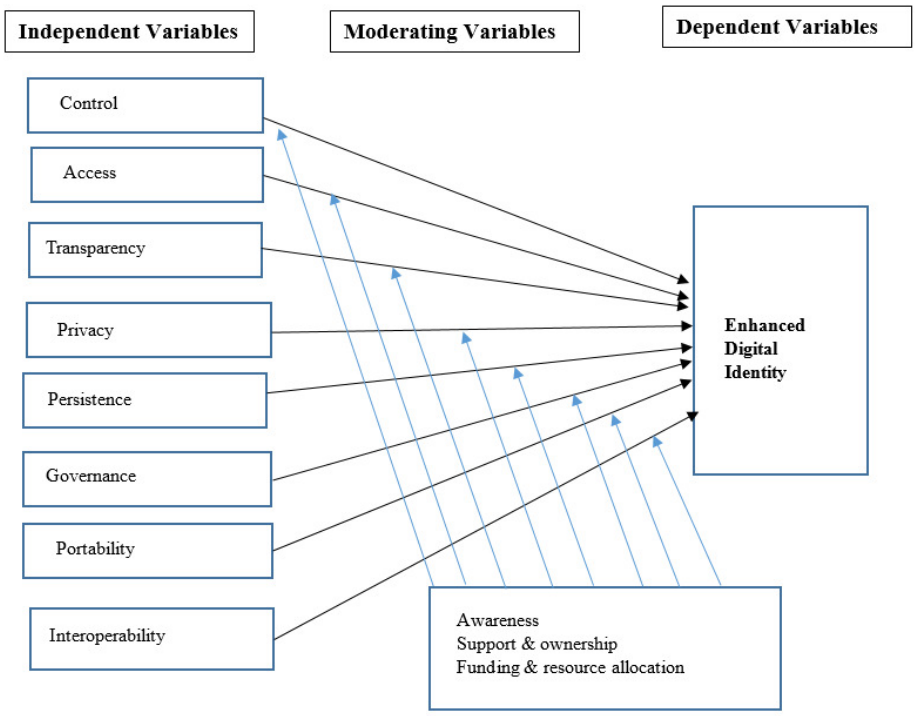

Figure 11: Proposed model for enhanced digital identity

Definition of Model Constructs

a) Control -In this research refers to beneficiaries having ultimate authority to their identity whereby they can refer to it, update it and hide it. The identification services should give people real choice and control over how their data is collected and used. This includes the ability to select only the attributes required for a transaction.

b) Access - refers to the ability of a beneficiary to always have unrestricted access to their own data. Further, access to beneficiary identity between humanitarian agencies should be streamlined to reduce multiplicity and limit restrictions such as affordability.

c) Transparency- The humanitarian identity system for humanitarian aid is open to the public about how it functions and how it is managed and updated. They should use open standards and, ensure technology and vendor neutrality.

d) Privacy- Some recipients of benefits may feel ashamed about their perceived inability to provide for themselves. This can lead them to withdraw from social and political life.

Social security benefits recipients should have identity systems that are sensitive to the needs of the most vulnerable people.

e) Persistence – Refers to identities that are robust, unique, accurate, and long-lived. Preferably, all potential beneficiaries of social protection should be issued with a life-long identifier used during targeting and registration. Linkages with civil registries will further strengthen identity persistence, ensuring assistance goes to the proper beneficiary and eliminating chances of double dipping.

f) Governance – Creates an enabling environment for the digital identity systems to effectively and efficiently function. This is achieved by ensuring the availability of necessary legal frameworks, defining and assigning roles to stakeholders, and ensuring accountability. The governance model should provide mechanisms to address grievances among humanitarian actors whenever they arise.

g) Portability- Ensures beneficiary identities are not centrally managed by one humanitarian actor or third-party service provider. This mitigates the risk of loss of information and services when humanitarian organizations close projects in an area, government regime changes, or beneficiaries such as pastoralists move to different locations. The user can keep his identity safe with portable identities.

h) Interoperability -Allows identities to be widely used within the humanitarian sector, recognized by government institutions, and trusted by private institutions. Issued digital identities are not necessarily legal identities. However, since the issuing authority is trusted, beneficiaries without legal identities could use their digital identities to access government services, open bank accounts, and freely move within the country's borders.

Moderating variables

i) Awareness- is a factor in both the use and acceptance of any identity system. All stakeholders should be aware , accept and trust an identity system for it to be useful.

j) Support and Ownership- Participating agencies, government and beneficiaries who form the key stakeholders of the digital identity system need to establish structures and policies

to strengthen ownership and support for the system. Participating agencies should integrate digital identification of beneficiaries in all project implementations

k) Funding and resource allocation - Identity systems require adequate funding and resource allocation to be able to reach a larger population. Identification systems must be long-term sustainable in terms of fiscal and operational viability.

Table 5: Variable operational Table

Variable	**Evaluation Parameter**	**Description**
1. Control	Consent	The enhanced model requires beneficiary consent for the collection, use or disclosure of personal information.
	Accuracy	Beneficiary identities and profiles provided by the enhanced model are complete, accurate, and updated.
	Data rights	The enhanced model empowers beneficiaries to actively participate in management of their data
	Authentication	The enhanced model restricts access to beneficiary identities to only authorised persons
2. Access	Availability	The enhanced model shall provide beneficiaries easy access to their personal identities
	Affordability	The enhanced model accessible to all beneficiaries and within the available budget.
	Acceptability	All stakeholders recognize and mutually agree to deploy the enhanced digital identity model

3. Transparency	Informativeness	The enhanced model shall enhance quality of information shared
	Openness	Information on the technologies and management of personal information shall be readily available.
	Understandability	Information shared by the enhanced model will be in a user friendly format
4. Privacy	Data minimization	The amount of personally identifiable information collected by the enhanced model shall be kept to a strict minimum.
	Privacy by design	Privacy by Design is embedded into the design and architecture of the enhanced model.
	Security	The enhanced model will ensure beneficiary identities are secure in storage and transit
5. Persistence	Longevity	Identities provided by the enhanced model shall be long-lived
	Censorship resistant	The enhanced model will issue immutable identities
	Force-resilient	The performance of the enhanced model should be able to deal with damages
	Decentralization	The enhanced model adopts distributed algorithms to manage identities
6. Governance	Compliance	Necessary steps to monitor, evaluate, and verify compliance with identification policies and procedures should be taken.

	Accountability	Assign responsibilities to ensure identification standards, policies and procedures are in place and adhered to.
	Funding	Providing all the necessary resources
	Ownership and Support	Management encouragement and ownership
7. Portability	Transportability	Ability to physically move software and associated artifacts, whether by means of transportable media or a network
	Vendor lock-in	The enhanced digital identity model should prevent Vendor lock-in
	Technology lock -in	The enhanced digital identity model should prevent technology lock-in
8. Interoperability	Universality	Identities issued by the enhanced model are applicable to all stakeholders in the humanitarian sector
	Linkages with other registries	The enhanced model supports linkages with other registries

CHAPTER THREE: RESEARCH METHODOLOGY

3.1. Research Design

The research was conducted to test the hypothesis that were derived from the proposed enhanced digital identity model. Hypothesis testing allows for a better understanding of the relationships between variables. Survey and observation techniques were deployed to collect data through the use of questionnaires.

This research used both descriptive as well as explanatory research designs. Descriptive research is used to observe, describe and document relevant aspects of a situation in its natural state. A descriptive research design was chosen to analyze digital identity systems used in Kenya's humanitarian sector.

The explanatory research provides clarity to a research problem. Further, explanatory research provides an in-depth cause and effect analysis of the research topic. The explanatory research design was deployed to determine factors and the domains that affect digital identity systems in the humanitarian sector in Kenya.

This study also deployed a survey design through interviewing humanitarian agency staff and members of technical working groups involved in beneficiary targeting and registration. A preliminary study was done to identify the main barriers and drivers of digital identity within the humanitarian sector. The responses from questionnaires were coded to allow for analysis and hypothesis testing to propose an enhanced digital identity model within Kenya's humanitarian agencies.

3.2. Target Population

The target population consisted of humanitarian actors who directly use digital identity systems to complete their tasks. This included senior management, program managers, project coordinators, IT staff, field officers, and monitoring and evaluation officers. The population also included members of information technology working groups focused on beneficiary digital identity within the humanitarian sector.

3.3. Sample and Sampling size

Sampling was defined by Kumar & Phrommathed (2005) as the systematic process of selecting a group of elements out of a huge population. This enables estimating the characteristics of larger population elements.

This study used a purposeful random sample of the target population. Purposefully random sampling is used to identify a population that are not aware about the research outcome. It seeks to achieve dependable and trustworthy findings.

The study was able to maintain a manageable sample size without affecting the quality of the findings. It also minimized the costs of time, money, and human resources. Yamane (1967) provides a simplified method to calculate sample sizes.

$$n = \frac{N}{1+Ne^2}$$

Where

n = Sample size

N = Population size

e = Margin of error (MoE)

$$n = \frac{90}{1+90(0.05)_2} = 74$$

3.4 . Data Collection

Data collection is the process of collecting information to answer a research question. The study utilizes questionnaires as the data collection tool. The questionnaires are easy to administer and have a high rate of response. If presented consistently, they can also be used to reduce biasness.

3.5. Pilot Study

A pretest consisting of 50% of the sample size was undertaken to ensure that the questions' content, wording, sequence, format, and layout are logical, clear, and understandable. The pre-study helped to determine the most appropriate scale range.

3.6. Ethical Issues

The respondents were briefed on the purpose of the study and its aim. There was also a letter from the university to validate the research. Involvement in the study was voluntarily with respondents having an option to opt-out. No respondent was required to disclose their names thus protecting their identity and ensure anonymity.

3.7. Data Analysis

3.7.1. Data Preparation

Collected data was prepared for analysis using the outlined procedure:

- The questionnaires were reviewed to remove incomplete questionnaires
- Data cleaning was done to rectify inconsistent and ambiguous responses.
- Data coding was done to allocate numeric codes so that statistical techniques can be applied.

3.7.2. Methods of Testing Hypotheses and Analyzing Data

Descriptive analysis was utilized to compute percentages, measures of central tendency (mean, mode, median, and median), and measures of variability (range, standard deviation, and variance).

Linear regression was used to test the relationship between the independent variables and the dependent variable. Cronbach's Alpha was used for reliability which is the degree to which the measure of a construct is dependable. Construct validity was conducted to measure the extent to which a measure effectively represents the underlying construct that it is supposed to measure.

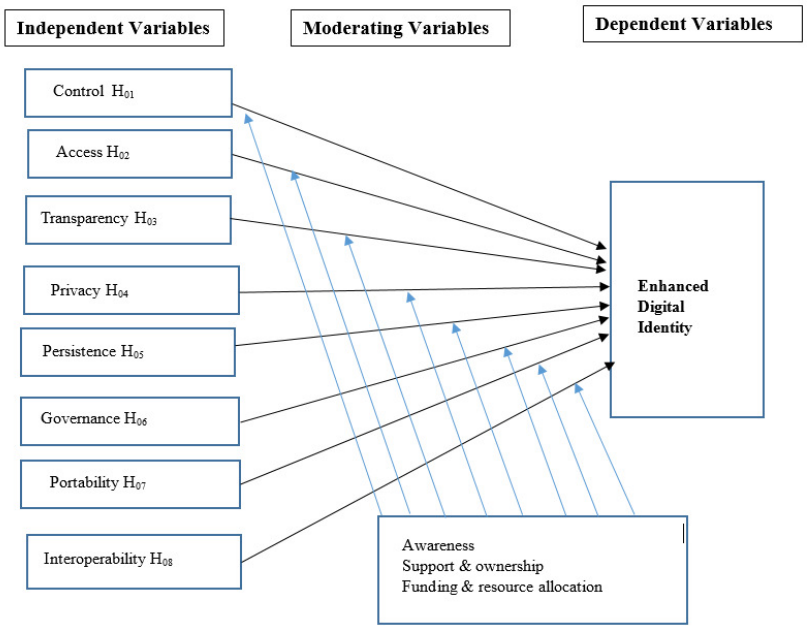

Figure 12: Operationalized Model

Operationalized Model through Hypothesis Testing

H01: Control has a direct effect on digital identities in the Humanitarian sector in Kenya

H02: Access has a direct effect on digital identities in the humanitarian sector in Kenya

H03: Transparency has a direct effect on digital identities in the humanitarian sector in Kenya

H04: Privacy has a direct effect on digital identities in the humanitarian sector in Kenya

H05: Persistence has a direct effect on digital identities in the humanitarian sector in Kenya

H06: Governance has a direct effect on digital identities in the humanitarian sector in Kenya

H07: Portability has a direct effect on digital identities in the humanitarian sector in Kenya

H08: Interoperability has a direct effect on digital identities in the humanitarian sector in Kenya

CHAPTER FOUR: RESULTS AND DISCUSSIONS

4.1 Introduction

The results and discussions chapter focuses on data analysis and interpretation of the findings.

4.2 Response rate

74 Questionnaires were administered to various consenting respondents drawn from different roles with varying years of experience and ages. Mugenda & Mugenda (2004) states that a response rate of more than 80% of the administered questionnaires is sufficient. In contrast, the study achieved a return rate of 100% as all 74 questionnaires were returned. The high response rate was achieved though frequent follow ups to ensure the questionnaires' completeness during the data collection exercise.

4.3 Demographic Characteristics

This section covers the respondents characteristics aggregated using descriptive statistics to analyze and present findings.

4.3.1 Organizational Roles of Respondents

Figure 13 below shows that majority of the participants in the survey were Field officers while Project Coordinators were the least. This indicates a great response to the study from various roles in the information system spectrum.

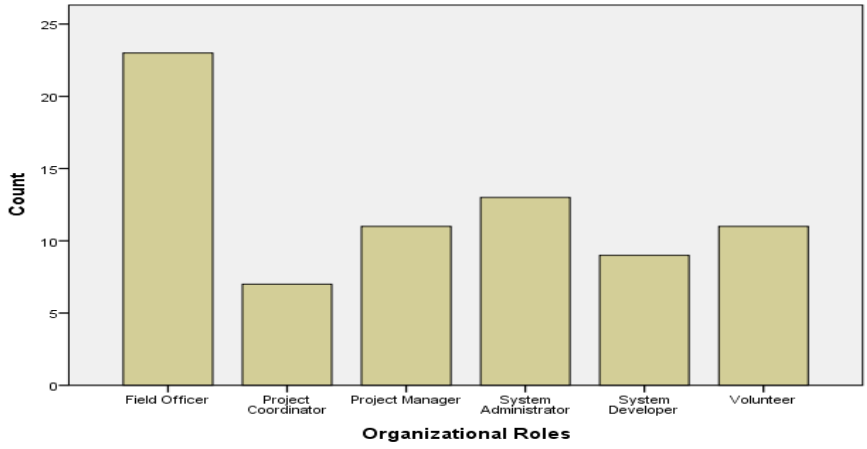

Figure 13: Organizational Roles of Respondents

4.3.2 Years of Experience

Most respondents, 79.7%, had more than three years of experience. One respondent reported 18 years, while seven others had only one year. The modal years were three and five years, respectively. Most respondents had sufficient years of experience to participate objectively in the study.

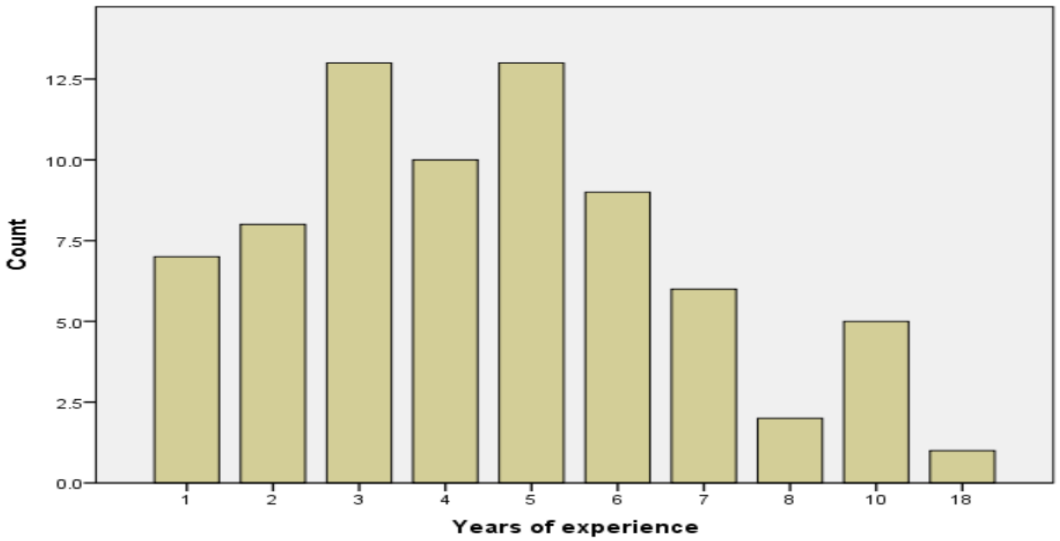

Figure 14: Number of years Worked

4.4. Pilot Study Results

A pilot study was conducted to identify and correct any errors in the questionnaire design before administering the main survey (Bell, 2014). This allowed for the validation and reliability testing of the tool.

4.4.1. Reliability of the research instrument

This is a measure of how likely a study instrument will produce consistent or unchanging results or information after repeated tests (Mugenda & Mugenda 2003). The coefficient alpha was used to determine the reliability and validity of the research instruments. Cronbach's alpha coefficients above 0.7 are acceptable and reliable (Hair Black, Babin & Anderson, 2010). Table 6 shows that the Cronbach alpha was 0.70 for each variable for standard items.

Table 6: Cronbach's Alpha Index

Construct	Cronbach's Alpha
Control	.856
Access	.836
Transparency	.839
Privacy	.794
Persistence	.811
Governance	.819
Portability	.849
Interoperability	.830

4.4.2. Validity of Research Instrument

Kaiser-Meyer-Olkin (KMO) was used to measure sampling adequacy and Bartlett's to test for sphericity of data before factor analysis. In table 7, the sample was acceptable since the KMO value was 0.792, which is above the 0.60 thresholds. This shows that the correlation pattern is relatively compact, so factor analysis should yield distinct and reliable factors (Hill, 2011). Likewise, the statistical significance was .000, which is acceptable.

Table 7: Sample Size Adequacy Test

KMO and Bartlett's Test

Kaiser-Meyer-Olkin Measure of Sampling Adequacy.		.792
Bartlett's Test of Sphericity	Approx. Chi-Square	1571.880
	df	325
	Sig.	.000

4.5 Variable Analysis

4.5.1 Digital Identity Control

Figure 15 below shows that almost 90% of respondents either agreed or strongly agreed that beneficiaries should freely consent to collect, use, and share their identities. 54% strongly agreed that beneficiaries' identities should be accurate, complete, and up-to-date. 88% either agreed or strongly agreed that beneficiaries have a right to actively participate in managing their identities. 92% agreed or strongly agreed that access to beneficiary identities should be restricted to authorized persons or entities.

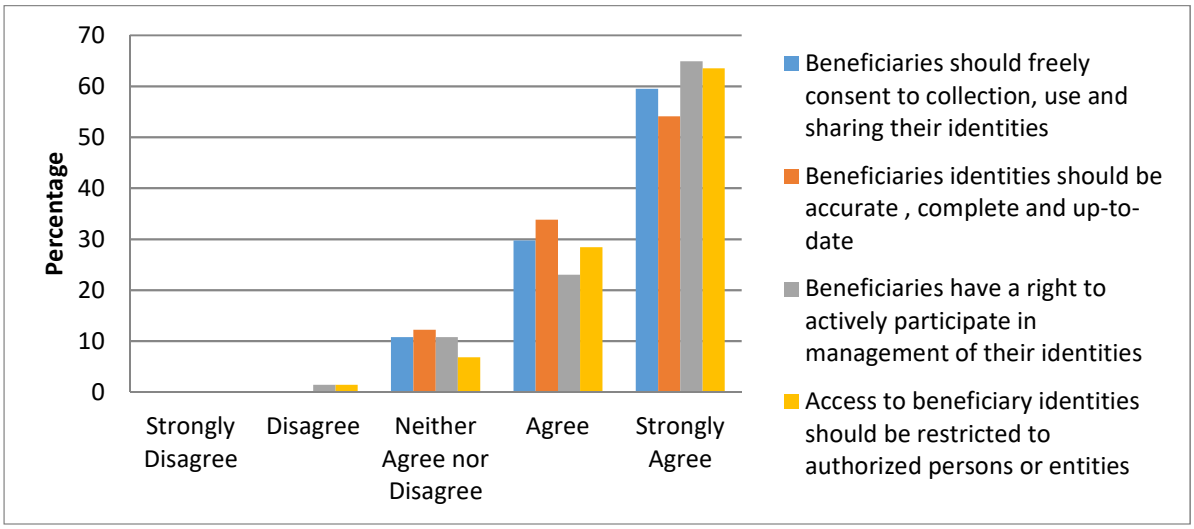

Figure 15: Control

4.5.2 Digital Identity Access

Similarly, 90% of the respondents agreed or strongly agreed that beneficiaries should be able to easily retrieve all data related to their digital identity. Likewise, 90% of respondents agreed or strongly agreed that the identity scheme should be accessible to all beneficiaries and at zero costs. 65% of the respondents strongly agreed that all humanitarian actors should recognize the enhanced digital identity scheme.

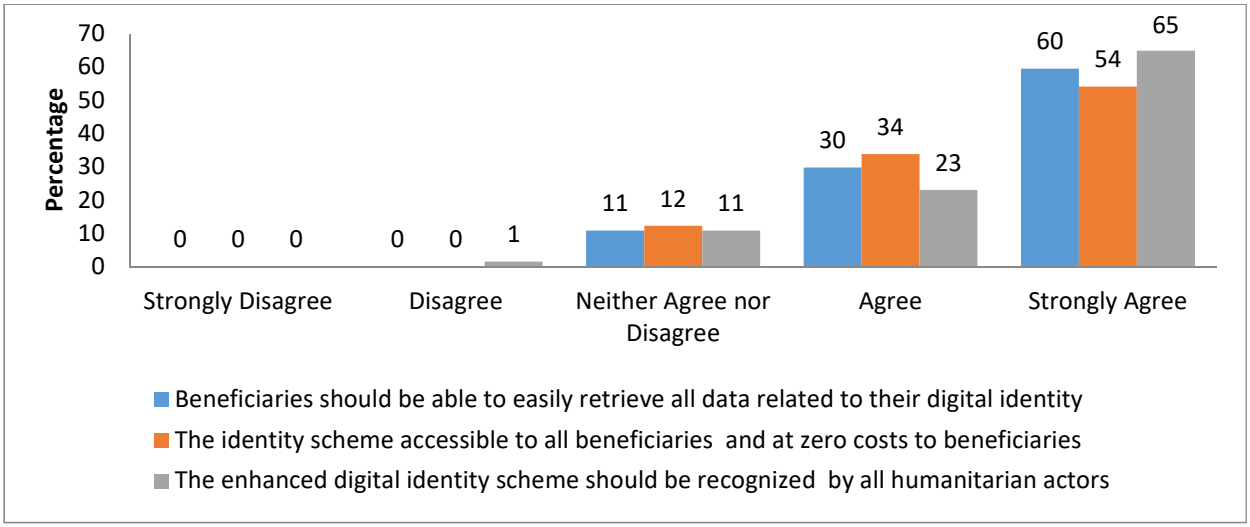

Figure 16: Digital Identity Access

4.5.3 Transparency

Figure 18 below shows that the majority, 86%, strongly agreed or agreed that digital identity systems should enhance the clarity and quality of beneficiary information shared. Likewise, 96% agreed or strongly agreed that digital identity systems must be open in how they are managed, function, and updated. 68% of the respondents strongly agreed that data rules and policies should be available in a user-friendly format. This shows how transparency of the digital identity is highly regarded.

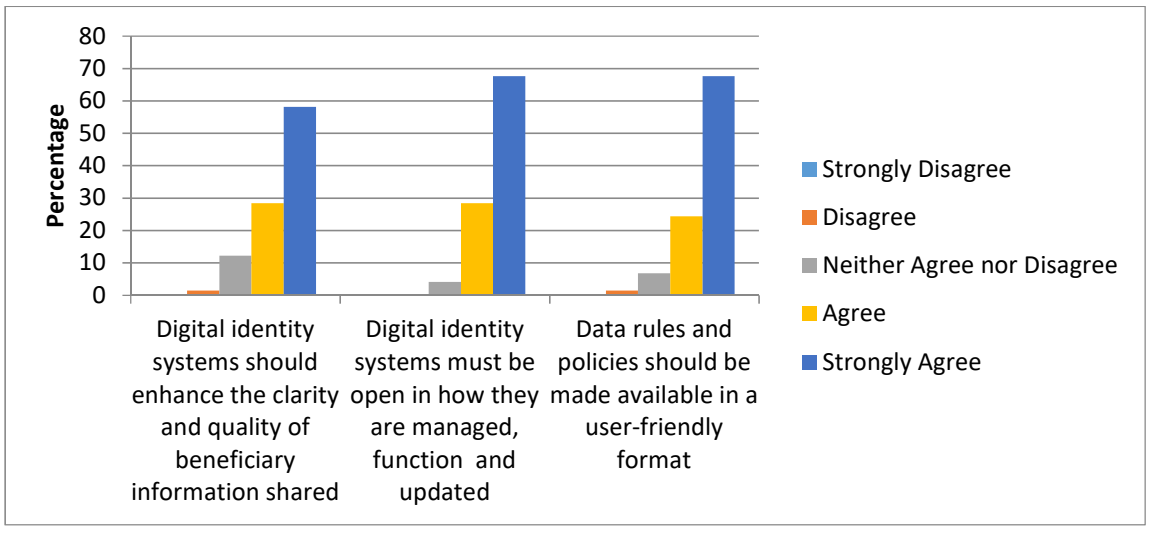

Figure 17: Transparency

4.5.4. Privacy

Digital Identity systems' limitation to the disclosure of personally identifiable information was supported by 87% who agreed or strongly agreed that it should be kept to a strict minimum necessary to ensure appropriate levels of assurance. Further, 84% agreed or strongly agreed that digital identity systems should incorporate privacy by design approaches. 89% agreed or strongly agreed that adequate safeguards should be in place to ensure the security of beneficiay identities.

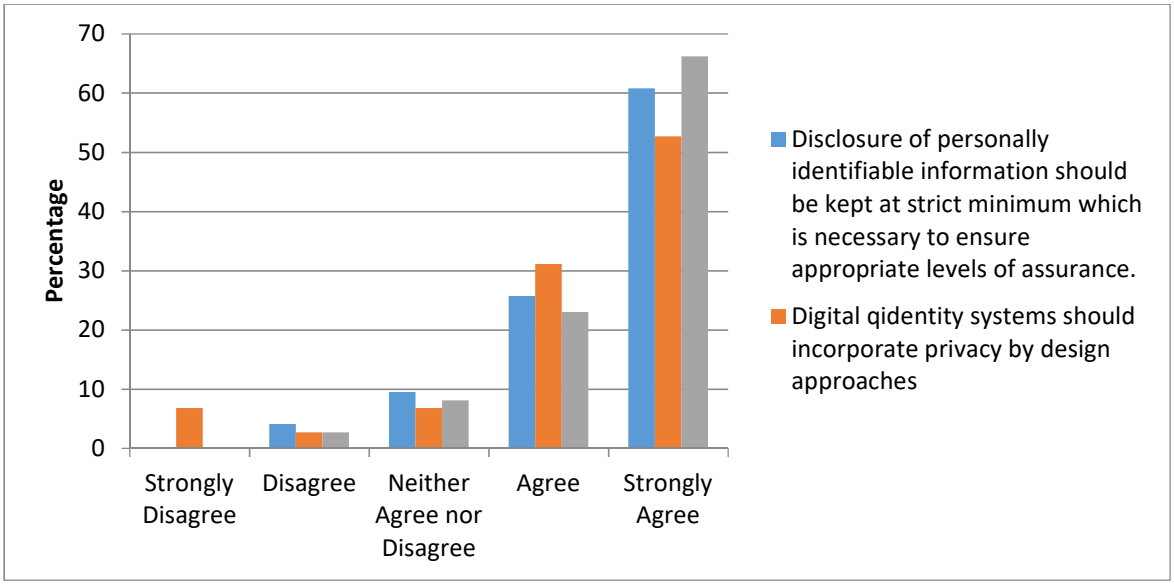

Figure 18: Privacy

4.5.5. Persistence

Most respondents, 51%, strongly agreed that digital identities must be long-lived, while 88% agreed or strongly agreed that digital identity authentication must occur through persistent censorship algorithms. A further 57% strongly agreed that digital identity authentication must occur through algorithms that are force-resilient, and a majority, 82%, agreed or strongly agreed that identity authentication must occur through algorithms that are run decentralized.

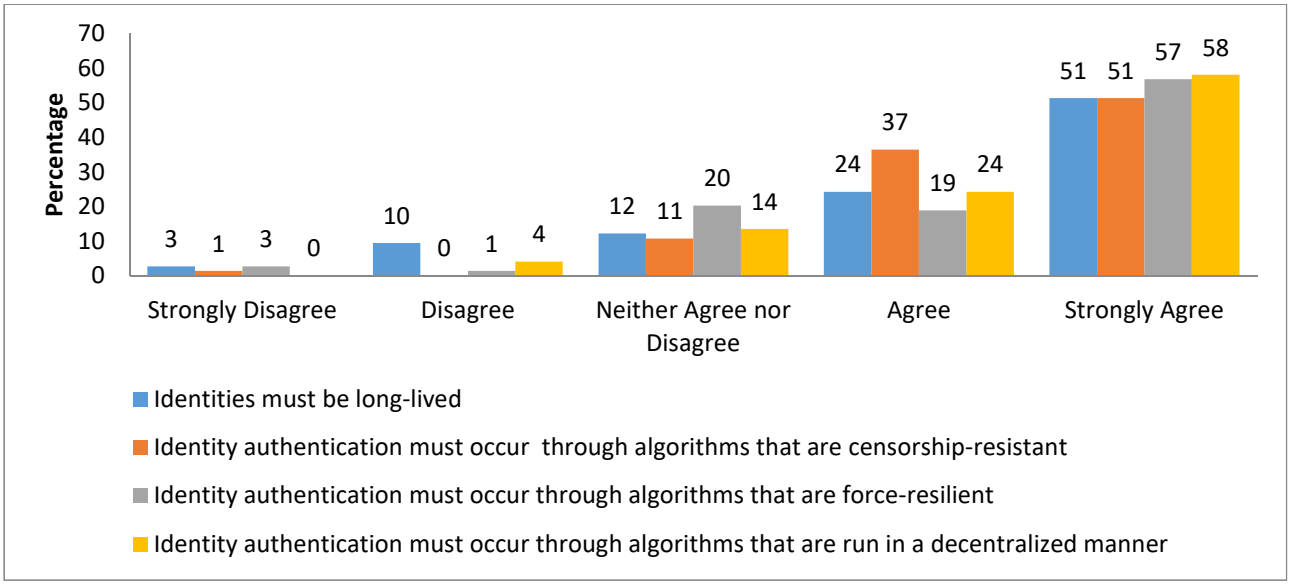

Figure 19: Persistence

4.5.6 Governance

91% agreed or strongly agreed that digital identity schemes should have mechanisms to verify, monitor, and evaluate compliance with identification standards and procedures. 90% agreed or strongly agreed that identity scheme stakeholders should be assigned roles and responsibilities in ensuring identification standards and procedures are in place and adhered to.

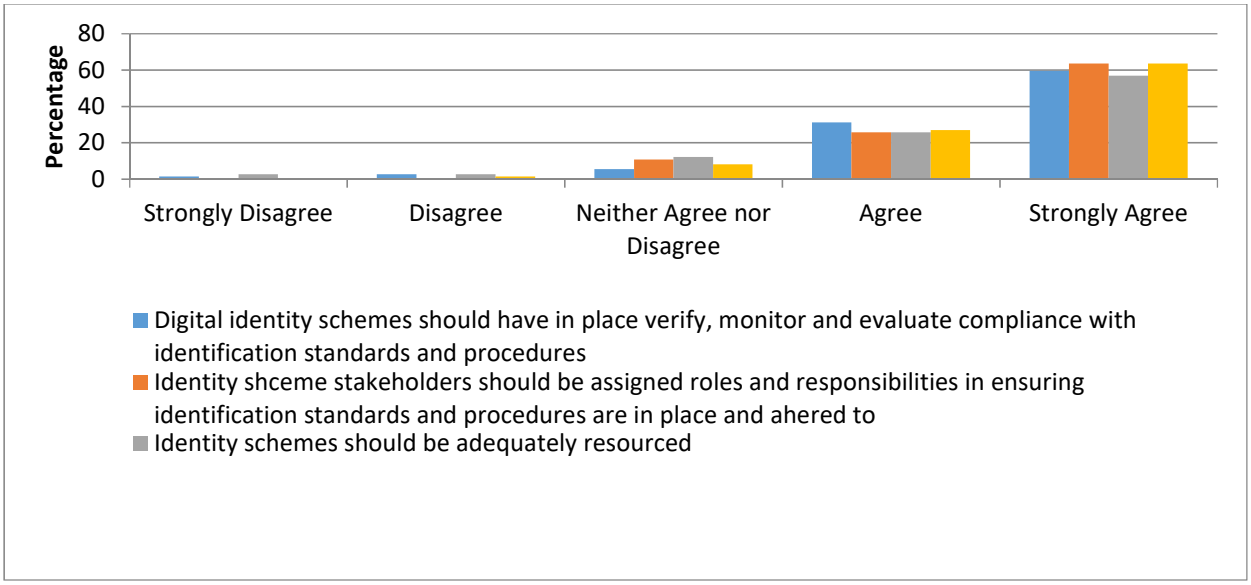

Figure 20: Governance

4.5.7. Portability

70% agreed or strongly agreed that information and services about identities should be moveable over a network or transportable media. And 89% agreed or strongly agreed that digital identity systems should adopt open standards and prevent vendor lock-in. A further 88% also agreed and strongly agreed that digital identity systems should adopt open standards and prevent technology lock-in.

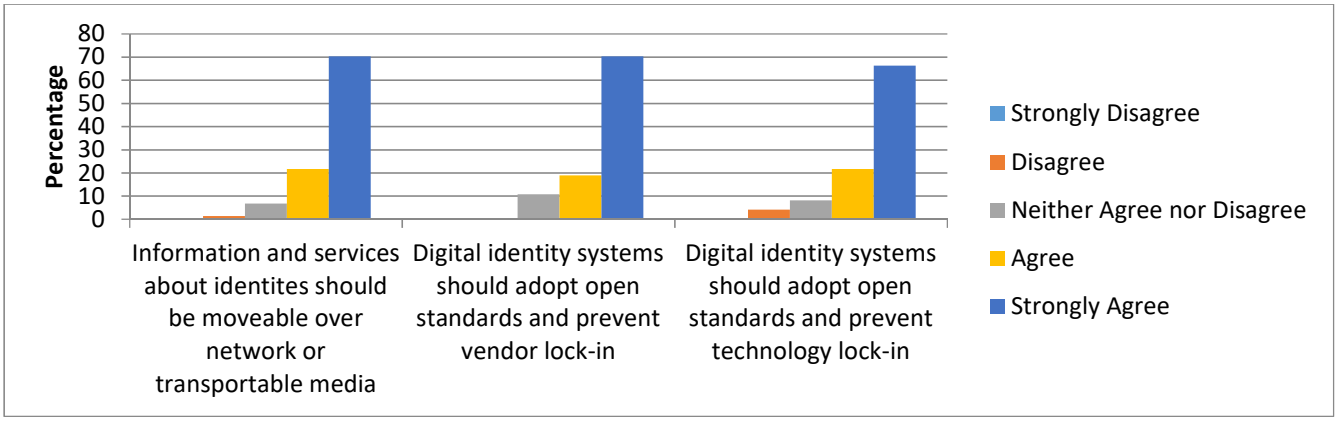

Figure 21: Portability

4.5.8. Interoperability

91% strongly agreed that digital identities should be as widely usable as possible. A similar percentage, 91%, also affirms interoperability as they agreed or strongly agreed that digital identification systems should be able to communicate with other systems, e.g., Civil registries and service providers.

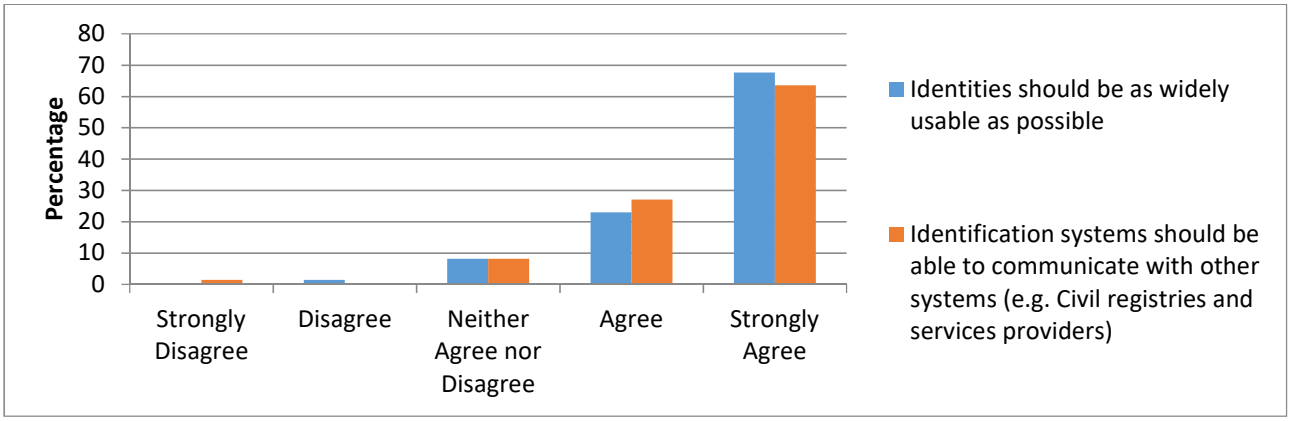

Figure 22: Interoperability

4.6. Factors Affecting Enhanced Digital Identity

4.6.1. Factors positively affecting digital Identities

The target respondents were required to give their input on whether they agreed on the drivers that would drive enhanced digital identity stemming from existing drivers as per literature. Most respondents strongly agreed that Digital Identity strengthened donor accountability, reduced fraud, allowed beneficiaries to control their identities, improved organizational efficiency, strengthened compliance with data protection regulations, and met competitive advantage.

Table 8: Digital Identity Drivers

Description	N	Mean	Std. Deviation
Strengthened accountability to donors	74	4.47	.763
Reduction in fraud and double dipping	74	4.45	.724
Beneficiary ability to control their identities	74	4.34	.911
Improved organizational efficiency	74	4.58	.662
Compliance with data protection regulations	74	4.51	.726
Meet competitive advantage	74	4.57	.704

4.6.2. Digital Identity Barriers

The participants were asked to weigh in on the barriers to Digital Identity. The results shown in the table below indicate that most respondents strongly agreed that lack of understanding of digital identities, lack of organizational policies and procedures to guide digital identity programs, short-term projects, lack of adequate resources to implement a digital identity program, data protection, and security risks and complex beneficiary targeting and registration process were all cited as barriers to digital identities.

Table 9: Digital Identity Barrier

Description	N	Mean	Std. Deviation
Lack of understanding on digital identities	74	4.18	1.038
Lack of organizational policies and procedures to guide on digital identity programs	74	4.35	.766
Short term projects (i.e. no return for investment and limited time to implement digital identity schemes)	74	4.27	.911
Lack of adequate resources to implement a digital identity program	74	4.28	.929
Data protection and security risks	74	4.23	.973
Complex beneficiary targeting and registration process	74	4.28	.958

4.7. Hypothesis Testing

The model summary results are as shown in the table below. We find that the R^2 is 0.880 while the adjusted R^2 is 0.865 which means that eighty-eight percent of the observed variation may be explained using linear regression.

Table 10: The Enhanced Digital Identity Model Summary

Model Summary

Model	R	R Square	Adjusted R Square	Std. Error of the Estimate
1	.938[a]	.880	.865	.23634

a. Predictors: (Constant), Interoperability, Governance, Persistence, Transparency, Privacy, Portability, Access, Control

Table 11: The enhanced digital identity model ANOVA

ANOVA[a]

Model		Sum of Squares	df	Mean Square	F	Sig.
1	Regression	26.589	8	3.324	59.502	.000[b]
	Residual	3.631	65	.056		
	Total	30.220	73			

a. Dependent Variable: Digital Identity

b. Predictors: (Constant), Interoperability, Governance, Persistence, Transparency, Privacy, Portability, Access, Control

Table 12: The enhanced Digital Identity model Coefficients

Coefficients[a]

Model		Unstandardized Coefficients		Standardized Coefficients	t	Sig.
		B	Std. Error	Beta		
1	(Constant)	-.041	.272		-.150	.881
	Control	.098	.103	.086	.948	.347
	Access	-.374	.090	-.356	-4.164	.000
	Transparency	-.049	.082	-.043	-.604	.548
	Privacy	.199	.063	.233	3.154	.002
	Persistence	.131	.061	.168	2.140	.036
	Governance	.227	.070	.213	3.250	.002
	Portability	.129	.091	.117	1.423	.160
	Interoperability	.661	.058	.684	11.481	.000

a. Dependent Variable: Digital Identity

The ANOVA table, table 11, above shows that the proposed Enhanced Digital Identity model is statistically significant at 0.000 and can predict the model's outcome better than chance.

Table 12 on Coefficients shows that Access, Privacy, Persistence, Governance, and Interoperability are the factors that significantly affect Enhanced Digital Identity. Access was the only negative predictor of enhanced digital identity. This means that as the access increases, the enhanced digital identity decreases. Privacy, Persistance, Governance, and Interoperability were positive predictors; hence as they increase, enhanced digital identity also increases, and their decrease also results in the decrease of the enhanced digital identity.

Concerning moderating variables, the relationships are measured by Beta values, representing the relationship's strength. The Beta values should not be less than 0.1; if they go beyond 1, there is a sign of Multicollinearity.

Table 13: Moderating variable analysis

	Awareness (Beta)	Support and ownership (Beta)	Funding and resource allocation (Beta)
Control	0.195	0.155	0.168
Access	0.156	0.141	0.206
Transparency	0.144	0.150	0.121
Privacy	0.111	0.118	0.163
Persistence	0.176	0.192	0.141
Governance	0.110	0.101	0.251
Portability	0.124	0.199	0.142
Interoperability	0.135	0.200	0.148

From the above summary, awareness, support and ownership, and funding and resource allocation had beta values above 0.1; therefore, they moderate all the independent variables.

Table 14 below indicates the hypothesis test and whether to reject or accept the hypothesis concerning the main variables in relation to the enhanced digital identity model. From the table, a probability of less than 5% means acceptance of Access, Privacy, Persistance, Governance, and Interoperability

H_{01}: Control has a significant role in digital identity

H_{02}: Access has a significant role in digital identity

H_{03}: Transparency has a significant role in digital identity

H_{04}: Privacy has a significant role in digital identity

H_{05}: Persistence has a significant role in digital identity

H_{06}: Governance has a significant role in digital identity

H_{07}: Portability has a significant role in digital identity

H_{08}: Interoperability has a significant role in digital identity

Table 14: Variable Test Summary Model

Hypothesis	**coefficient**	**t-statistic**	**p-value**	**Decision**
H_{02}: Access has a significant role in digital identity	-.356	-4.164	.000	Accept
H_{04}: Privacy has a significant role in digital identity	.233	3.154	.002	Accept
H_{05}: Persistence has a significant role in digital identity	.168	2.140	.036	Accept
H_{06}: Governance has a significant role in digital identity	.213	3.250	.002	Accept
H_{08}: Interoperability has a significant role in digital identity	.684	11.481	.000	Accept
H_{01}: Control has a significant role in digital identity	.086	.948	.347	Reject
H_{03}: Transparency has a significant role in digital identity	-.043	-.604	.548	Reject
H_{07}: Portability has a significant role in digital identity	.117	1.423	.160	Reject

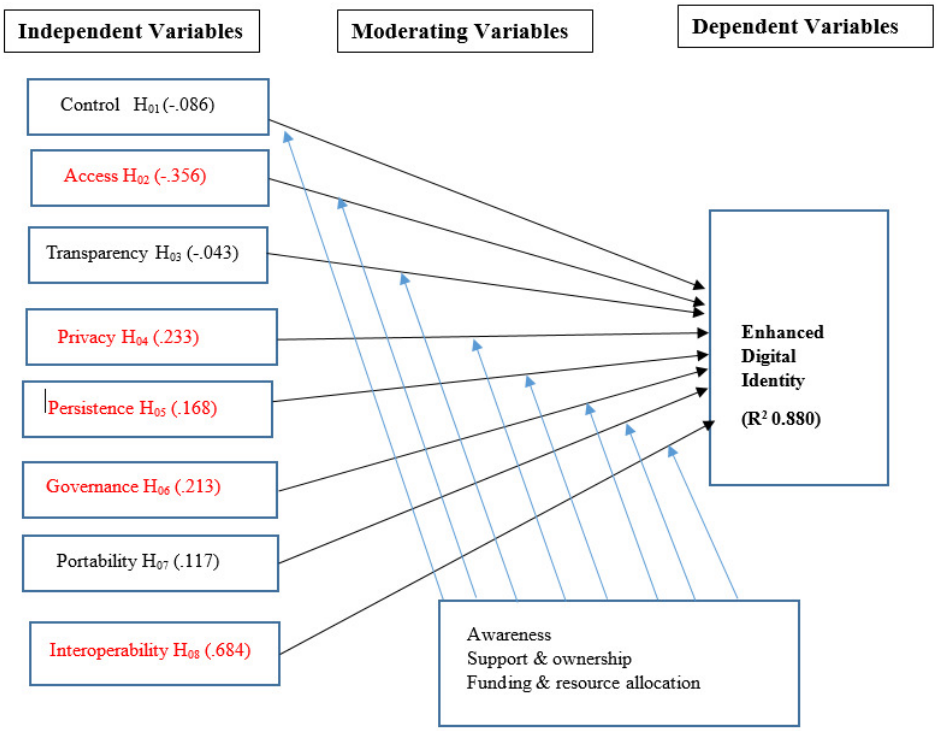

Figure 23:Hypothesis testing summary

CHAPTER FIVE : CONCLUSION & RECOMMENDATION

This chapter gives a synopsis of the results of the research in relation to the objectives, scope and constructs of the study.

5.1 Study Achievement

This research aims to develop an enhanced digital identity model for beneficiary targeting and registration. Eight variables were identified from the literature review. The variables directly impacted the digital identification of beneficiaries in humanitarian organizations in Kenya. The variables include; control, access, transparency, privacy, persistence, portability, governance, and interoperability. The proposed conceptual model represented the observable connections.

Research Objective 1 - Analyze identity trends in the humanitarian sector in Kenya.

Individuals or entities must identify themselves before receiving any service in the public or private sector. In the Humanitarian sector, beneficiary targeting, identification, and verification is a critical phase of project implementation which is time-consuming and requires significant funding. Beneficiary information is instrumental in project planning, decision making, and implementation. Also, identification of beneficiaries is mandatory before delivery of assistance. Unique identification of beneficiaries eliminates fraud, supports the deduplication process, and strengthens accountability.

Humanitarian agencies have long used paper-based methods to capture and store beneficiary information, including sensitive information such as vulnerabilities and health records. Paper-based methods are prone to error, data breaches, damages, and data loss, exposing organizations to financial and reputational risks. Poor record-keeping methods make retrieving beneficiary records difficult, delaying the reporting process.

Most organizations have migrated to using automated IT tools due to the limitations of paper-based methods. Furthermore, donors and development partners require accountability, transparency, and standardization of processes, which pushes agencies to use innovative solutions. Institutions with limited funding and short-term projects use simplified tools such as excel files and access databases to manage their beneficiary records. An iding scheme is applied to identify

each beneficiary, and formulas are applied to deduplicate uniquely. Also, project committees at the community level help with the identity proofing of beneficiaries.

The growing interest in digitization has led to establishing an innovation kitty from which tools such as WFP's SCOPE system, World Vision's Last Mile Mobile Solutions (LMMS), and UNHCR's Beneficiary Information Management tools have been developed. Similarly, for-profit institutions have also developed an interest in the humanitarian sector, thus developing software as a service tools such as RedRose, Salesforce, Mastercard Foundation Electronic Voucher system, and Commcare.

Identity systems have adopted sophisticated identity proofing and authentication mechanism such as biometrics to ensure assistance goes to the right beneficiary. With increased funding going into consortiums, organizations require tools with multi-agency capabilities to reduce duplication of efforts and effectively utilize funds allocated for building identity tools.

Data privacy and security are an increasing concern among humanitarian actors. Working groups and partners have developed manuals and tools such as the EU General Data Protection Regulations (GDPR), Oxfam, and ICRC Data Security and Privacy manuals, which support organizations in adopting and implementing measures to protect beneficiary data. Legal requirements, including transborder laws, continue to hinder data exchange across borders, considering that most donors are external institutions.

The identity ecosystem in Kenya has made significant strides in developing and adopting digital identities. Huduma Namba, Social protection Single registries, National Integrated Identity Management System (NIIMS), and Digital credit are some of the initiatives contributing to the new shift in identities, with all looking towards a single source of truth for identities. New and advanced technologies such as blockchain are immutable and provide peer-to-peer collaboration allowing service providers to quickly and accurately authenticate individuals.

Research Objective 2- Identify the factors affecting identity systems in the humanitarian sector in Kenya

The study results showed that the main reasons organizations adopt digital identity schemes are strengthened accountability to donors, reduced fraud and double dipping, the ability to control

their identities, improved organizational efficiency, compliance with data protection regulations, and meeting competitive advantage.

Further, the study identified a lack of understanding of digital identities, lack of organizational policies and procedures to guide digital identity programs, short-term projects, lack of adequate resources to implement a digital identity program, data protection and security risks, and complex beneficiary targeting and registration process as the barriers to digital identities.

Research Objective 3 - Propose an enhanced digital identity model for beneficiary targeting and registration for Humanitarian actors in Kenya.

The study proposed beneficiary access to their digital identities as well as privacy, persistence, governance, and interoperability as the key components when designing a digital identity program. All identification systems must be free of discrimination by policy, practice, and design. Identities should be available to everyone. It includes obligations and commitments to provide proof of identity to refugees, stateless persons, and migrants who don't have valid credentials or can't prove their legal identity. Technology gaps and costs should not prevent people from obtaining the identity credentials they need to access basic rights and entitlements.

Protecting personally identifiable information from misuse must be done proactively and automatically through a strong legal framework, system design, and the adoption of technical standards. Global norms regarding data protection should be adhered to in the design, policies, and technology used for identification systems. Authentication protocols should disclose only the minimal data required to provide appropriate levels of security and keep data as short as necessary for lawful use or consent purposes.

People should have the right to choose and control how their data is used. They should also be able to select the attributes necessary for any transaction. Governance frameworks must strike a balance between self-regulatory and regulatory models so they do not hinder innovation, competition, or investment. Cross-border interoperability and mutual recognition require appropriate legal and regulatory frameworks.

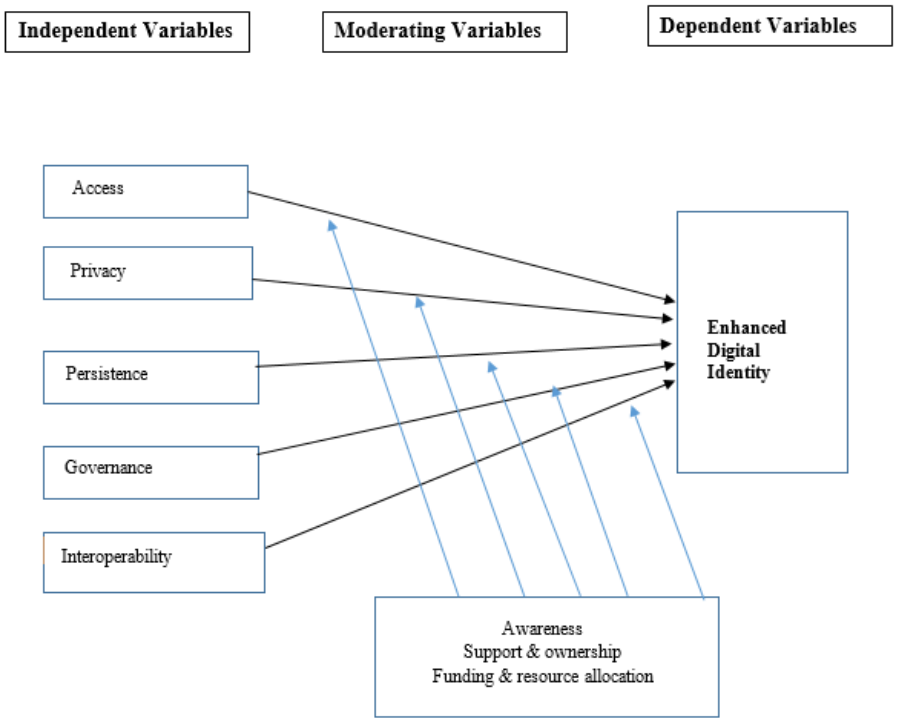

Figure 24: Enhanced digital Identity Model for Humanitarian Agencies in Kenya

5.2. Study Limitation

Research shortcomings may arise from the study's methodology, participants, or procedures. The study was limited to beneficiaries under humanitarian interventions through the non-governmental organization in Kenya. Also, the study focused on input from project staff only though beneficiary identity schemes that also affect beneficiaries.

5.3. Future Direction

It will be necessary for the future to build a more robust digital identification model based on the suggested extensions. Secondly, a similar study must focus on the development sector. This will strengthen the interoperability of digital identities and linkages with other systems.

5.4. Conclusion & Recommendation

Adopting the enhanced digital identity model will ensure that humanitarian organizations' identification systems are accessible to all beneficiaries without discrimination and employ adequate privacy safeguards during the design and architecture stage. Also, the identities are

persistent in supporting long- and short-term projects and addressing duplicity and falsification of documents.

Enhanced digital identity model will promote good governance of identities within the humanitarian sector. Interoperability will strengthen linkages with other registries, including civil registries, ultimately ensuring beneficiaries can acquire legal identities which enable them to access government services.

Humanitarian actors should jointly build a digital identity system based on the enhanced digital identity model. In addition, beneficiaries should be involved in the design and improvement of the model and future system development.

REFERENCES

Alemayehu, C., & Mwangi, J. (2011). *An Interoperable Identity Management Solution for Kenya E-Government*.

Allen, C. (2016). *The Path to Self-Sovereign Identity*. http://www.lifewithalacrity.com/2016/04/the-path-to-self-soverereign-identity.html

Alsayed Kassem, J., Sayeed, S., Marco-Gisbert, H., Pervez, Z., & Dahal, K. (2019). DNS-IdM: A blockchain identity management system to secure personal data sharing in a network. *Applied Sciences*, *9*(15), 2953.

CAJ. (2015). *HATA MNYONGE ANA HAKI, STATELESS IN KENYA AN INVESTIGATION REPORT ON THE CRISIS OF ACQUIRING IDENTIFICATION DOCUMENTS IN KENYA*. the Commission on Administrative Justice.

Domingo, A. I. S., & Enriquez, A. M. (2018). Digital Identity: The current state of affairs. *BBVA Research*, 1–46.

Dylan Yaga, K. S., Peter Mell, Nikx Roby. (2018). *NISTIR 8202, Blockchain Technology Overview*. National Institute of Standards and Technology.

Gardner, C. (2020). *Opportunities of, and obstacles to, the utilisation of the Enhanced Single Registry, Kenya Social Protection Research Study 1*.

Geteloma, V., Ayo, C. K., & Goddy-Wurlu, R. N. (2019). *A Proposed Unified Digital Id Framework for Access to Electronic Government Services*. *1378*(4).

Gok. (2018). *Integrated population registration system (IPRS)*. https://www.immigration.go.ke/integrated-population-registration-systemiprs/

GoK. (2021). *Huduma Namba*. https://www.hudumanamba.go.ke/

Grassi, P. A., Garcia, M. E., & Fenton, J. L. (2017). NIST special publication 800-63-3 digital identity guidelines. *National Institute of Standards and Technology, Los Altos, CA*.

ITU-T. (2017). *ITU-T Focus Group Digital Financial Services, Identity and Authentication*. International Telecommunication Union (ITU).

ITU-T. X.1252. (2010). *SERIES X: DATA NETWORKS, OPEN SYSTEMCOMMUNICATIONS AND SECURITY, Cyberspace security – Identity management ,Baseline identity management terms anddefinitions*. International Telecommunication Union.

ITU-T X.1254. (2021). *SERIES X: DATA NETWORKS, OPEN SYSTEM COMMUNICATIONS AND SECURITYCyberspace security – Identity management, X.1254*. International Telecommunication Union (ITU).

Mugenda, O. M., & Mugenda, A. G. (2003). *Research Methods, Quantitative and Qualitative Approaches*. ACT.

Mühle, A., Grüner, A., Gayvoronskaya, T., & Meinel, C. (2018). A survey on essential components of a self-sovereign identity. *Computer Science Review*, *30*, 80–86.

Muthuri, R. (2018). *BIOMETRIC TECHNOLOGY, ELECTIONS, AND PRIVACY, INVESTIGATING PRIVACY IMPLICATIONS OF BIOMETRIC VOTER REGISTRATION IN KENYA'S 2017 ELECTION PROCESS.*

Naik, N., & Jenkins, P. (2020). Self-Sovereign Identity Specifications: Govern your identity through your digital wallet using blockchain technology. *2020 8th IEEE International Conference on Mobile Cloud Computing, Services, and Engineering (MobileCloud)*, 90–95.

Schoemakert, K. (2019). *Kenya's Identity Ecosystem*. Caribou Digital.

Slavin, A. (2019). Distributed ledger identification systems in the humanitarian sector. *Sovrin Foundation. May*.

Stokkink, Q., & Pouwelse, J. (2018). Deployment of a blockchain-based self-sovereign identity. *2018 IEEE International Conference on Internet of Things (IThings) and IEEE Green Computing and Communications (GreenCom) and IEEE Cyber, Physical and Social Computing (CPSCom) and IEEE Smart Data (SmartData)*, 1336–1342.

USAID. (2018). *IDENTITY IN A DIGITAL AGE:INFRASTRUCTURE FORINCLUSIVE DEVELOPMENT*. USAID.

WFP. (2015). *Community-Based Targeting Guide*.

World Bank Group. (2021). *Principles on Identification for Sustainable Development: Toward the Digital Age—Second Edition (English)*.

Zheng, Z., Xie, S., Dai, H., Chen, X., & Wang, H. (2017). An overview of blockchain technology: Architecture, consensus, and future trends. *2017 IEEE International Congress on Big Data (BigData Congress)*, 557–564.

PRELIMINARY RESEARCH

1. In your own opinion what are the main drivers of adoption of digital identities in your organisation? (Please list as many as possible)

_____

_____

_____

_____

_____

_____

_____

2. In your own opinion what are the main bariers to adoption of digital identities in your organisation? (Please list as many as possible)

_____

_____

_____

_____

_____

_____

_____

_____

RESEARCH QUESTIONNAIRE

Part A: Cover Letter

Dear Volunteer,

My name is John Magaiwa Meng'anyi. I am currently a University of Nairobi student pursuing a Master of Information Technology Management. My study aims to create a digital identity model for Kenyan humanitarian agencies. This study will also help to understand identity trends in Kenya's social protection sector.

Digital identity refers to the digital representation of an entity that is detailed enough for the individual to be distinguishable in the digital context. A more accurate digital identity model will enable project staff to identify beneficiaries quickly, speed up distribution activities, strengthen accountability and improve organizational efficiency.

You are not obligated to take part in this. You are free to answer whichever questions you choose or stop participating altogether. By responding to this survey, you will not be personally identifiable. All replies will be tallied, summarized, and analyzed before a Master's degree is granted. If you are a study participant and need more information about your rights, you can contact the University of Nairobi Offices in Kenya. Send an email if you have questions about the questionnaire or the study to magaiwa@gmail.com

Please read the questions provided below and then answer them by ticking where appropriate.

1. Indicated that the above was read and comprehended. I'm happy to take part in this survey.. *

Yes ( )

No ( )

2. If No, Could you please explain the rationale? *

PART B: DEMOGRAPHICS

3. Gender

Male ( )

Female( )

4. What is your length of service in years to the company? *

5. Age *

6. Have you used any beneficiary digital identity solutions in your organization? *

Yes ( )

No ( )

7. When it comes to the company's IT infrastructure, which of the following best describes your responsibilities? *

a) Project Manager ( ) b) Project Coordinator ( ) c) Filed Officer ( )

d) System Administrator ( ) e) System Developer ( ) f) Volunteer ( )

g) Other specify ( )

	1= Strongly disagree 2= Disagree 3= Don't know 4= Agree 5= Strongly agree					
PART C: DIGITAL IDENTITY BARIERS Please rate the extent to which the following statements describe the circumstances under which your company would implement a formal digital identification system.		1	2	3	4	5
C07	Strengthened accountability to donors					
C08	Reduction in fraud and double dipping					
C09	Beneficiary ability to control their identities					

C10	Improved organizational efficiency					
C11	Compliance with data protection regulations					
C12	Meet competitive advantage					
Part D: Digital Identity Barriers Please rate how much you agree with the following statements about obstacles to implementing a digital identification system at your firm.		1	2	3	4	5
D13	Lack of understanding on digital identities					
D14	Lack of organizational policies and procedures to guide on digital identity programs					
D15	Short term projects (i.e. no return for investment and limited time to implement digital identity schemes)					
D16	Lack of adequate resources to implement a digital identity program					
D17	Data protection and security risks					
D18	Complex beneficiary targeting and registration process					
Part E: Control		1	2	3	4	5
E19	Beneficiaries should freely consent to collection, use and sharing their identities					
E20	Beneficiaries identities should be accurate , complete and up-to-date					
E21	Beneficiaries have a right to actively participate in management of their identities					
E22	Access to beneficiary identities should be restricted to authorized persons or entities					
Part F: Access		1	2	3	4	5
F23	Beneficiaries should be able to easily retrieve all data related to their digital identity					

F24	The identity scheme should be accessible to all beneficiaries and at zero costs to beneficiaries					
F25	The enhanced digital identity scheme should be recognized by humanitarian actors					
Part G: Transparency		1	2	3	4	5
G26	Digital identity systems should enhance the clarity and quality of beneficiary information shared					
G27	Digital identity systems must be open in how they are managed, function and updated					
G28	Data rules and policies should be made available in a user-friendly format					
Part H: Privacy		1	2	3	4	5
H29	Disclosure of personally identifiable information should be kept at strict minimum which is necessary to ensure appropriate levels of assurance.					
H30	Digital identity systems should incorporate privacy by design approaches					
H31	Adequate safe guards should be in place to ensure security of beneficiay identities					
Part I: Persistence		1	2	3	4	5
P132	Identities must be long-lived					
P133	Identity authentication must occur through algorithms that are censorship-resistant					
P134	Identity authentication must occur through algorithms that are force-resilient					
P135	Identity authentication must occur through algorithms that are run in a decentralized manner					
Part J: Governance		1	2	3	4	5

P136	Digital identity schemes should have mechanisms in place verify, monitor and evaluate compliance with identification standards and procedures					
P137	Identity scheme stakeholders should be assigned roles and responsibilities in ensuring identification standards and procedures are in place and ahered to					
P138	Identity schemes should be adequately resourced					
P139	Management should take ownership and support beneficiary digital identity initiatives					
Part K: Portability		1	2	3	4	5
P140	Information and services about identites should be moveable over network or transportable media					
P141	Digital identity systems should adopt open standards and prevent vendor lock-in					
P142	Digital identity systems should adopt open standards and prevent technology lock-in					
Part L: Interoperability		1	2	3	4	5
P143	Identities should be as widely usable as possible					
P144	Identification systems should be able to communicate and exchange data with other systems (e.g. Civil registries and services providers)					
Part M: Digital Identity		1	2	3	4	5
Dig1	Digital Identity systems should maximize ID coverage					
Dig2	Digital Identity systems should improve trust and end-user experience with identification					

Please indicate any other areas that you think should be included in an enhanced digital identity program for humanitarian agencies in Kenya?

_____

_____