Dignified ID in Cash Assistance in East Africa

In partnership with

Innovation Norway

NORWEGIAN CHURCH AID

NRC NORWEGIAN REFUGEE COUNCIL

Norwegian Red Cross

Save the Children

Written by:

Senka Hadzic | E4C Research Fellow | Cape Town, South Africa

Edited by:

Mariela Machado | E4C Program Manager | New York, NY, USA
Grace Burleson | E4C Jr Program Manager | Ann Arbor, MI, USA
Jennifer Ventrella | E4C Expert Fellow | New York, NY, USA

Additional contribution:

Pauline Mweu | Jr Research Fellow | Nairobi, Kenya
Giulio Coppi | Digital Specialist, Norwegian Refugee Council | Oslo, Norway

EXECUTIVE SUMMARY

With over 1 billion people worldwide lacking a form of legal identity, many individuals lack access to government and humanitarian services, and financial services particularly individuals in need of humanitarian assistance, such as refugees. Target 16.9 of the Sustainable Development Goals aims to address this need by providing institutionally-recognized identify for all by 2030. With the growing use of digital and mobile technologies worldwide, digital forms of legal identification could improve many populations' access to ID and other digital services. However, implementing a large-scale digital service involves a variety of stakeholders, including the government, service providers, implementers, communities, and individuals. For a digital ID solution to succeed, all stakeholders must be aligned and engaged.

To understand the role of stakeholders and their interactions with one another in a digital ID implementation, four key relationships are evaluated:

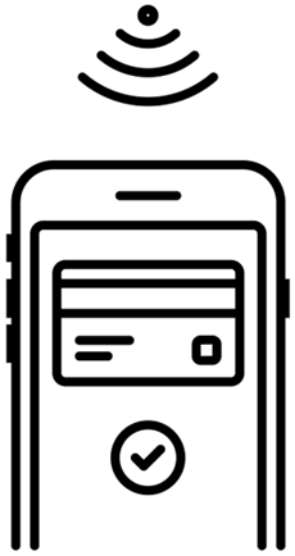
1. **Government to implementing organization:** An enabling regulatory environment is essential for digital ID solutions to succeed. NGOs and multilaterals that aim to implement a digital ID service must work alongside local and national governments to ensure policies of data protection and financial inclusivity exist.
2. **Service providers to individuals:** Designers of a digital ID solution must understand and incorporate their specific end user's context, which includes understanding their literacy rates, current notion of identity, trust in local authority, desires for convenience, consent practices, and cultural preferences; among others.
3. **Service provider to service provider:** Partnerships between service providers, particularly regarding the role of telecommunication companies, must include trust, data security, and plans for interoperability.
4. **Community to individual:** End users desire a quality service that meets their needs, is convenient to use, and operated by locally-accessible agents.

Digital interventions must be disseminated in enabling environments that allow the services to operate efficiently and ethically. Trends that enable successful digital ID solutions include (1) trust, (2) standards and policy, and (3) ICT infrastructure; in addition to overarching global initiatives and collaborations. And although providing an enabling environment is essential for successful implementation of a digital ID system, a strong contextual analysis regarding a digital ID system's user provision model is mandatory. We present a checklist to guide practitioners through the evaluation process required to design an appropriate user provision model, including integrating aspects of user value, local trust, convenience, standards, data security, and interoperability; among others.

Ultimately, the goal of implementers is to improve the lives of disadvantaged populations, who require access to services and local resources. With this in mind, a solution, whether it be digital or otherwise, must be robust, locally appropriate, and context-specific.

TABLE OF CONTENTS

Digital Identity: An Overview



According to the World Bank, over 1 billion people in the developing world lack proof of legal identity [1], which is a government-recognized form of designation to uniquely distinguish a particular person [2]. To address this global need, target 16.9 of the Sustainable Development Goals (SDGs) aims to

"provide legal identity for all, including birth registration, by 2030." [3]

With the growing use of digital and mobile technologies worldwide, many governments and institutions are looking at the use of digital solutions and technologies to achieve this target. Digital identity is an electronic representation of a person, including unique credential data (e.g. biometrics), that is managed by a local government, multilateral organization, or NGO, which is integrated into local processes and services, such as regional financial services and mobile infrastructure [2, 4]. There are two primary categories of ID systems, both of which are considered in this report: (1) legally recognized identity, such as national civil registries; and (2) contextual identity, which includes service-based systems such as voter registrations, health records, or status determination cards [5].

Digital ID can be complex to implement since the systems require meeting the needs of governments and policymakers all while working within the available telecommunications infrastructure, financial services, and other physical infrastructures. This complexity is aggravated when designing a program for undocumented individuals, which make up a substantial portion of the refugee populations worldwide. Although digital ID systems can help streamline operations through easier data collection and storage, create a more robust system of authenticated ID, and enable better access to services, these programs introduce unique challenges regarding data privacy and protection, lessened user agency, and issues of interoperability between organizations that use different technologies and data storage platforms.

While digital technologies (e.g. cloud computing, biometrics, and mobile apps) are thought to increase the security, accuracy, and convenience of identifying and authenticating individuals as compared to paper-based identification [6], it is important to note that technology amplifies pre-existing biases. Since the introduction of new technologies can lead to challenges and risks, especially when there is a lack of policy and regulatory frameworks, digital identification systems must be implemented strategically into a system that includes trust, protection of individuals, and reliable infrastructure.

Often, the incentive to introduce digital ID is to consolidate identification and financial resources into one platform. Even though mobile money services generally support financial inclusion of the world's underserved populations, individuals who lack an official form of identification are largely excluded from mobile money services, and women are disproportionately affected [6]. In Kenya, registration for SIM cards and mobile money platforms require identification, such as an original national identity card, passport, or birth certificate [7] and identity documents issued by humanitarian organizations (e.g. the UNHCR refugee card) are currently not an accepted form of identity for SIM registration [8]. As of late 2018, Kenya hosted over 460,000 registered refugees and asylum seekers, however, the Kenyan National Registration Bureau does not use the same ID number when renewing or reissuing a refugee ID card, creating ongoing complications for card holders [8].

Assessing the Landscape

Due to the complexities of integrating digital ID solutions into local systems, understanding of stakeholder roles is of utmost importance. Stakeholders and their relationships with one another make or break technology implementations.

Specifically, for digital ID solutions, key stakeholder groups include the government, service provider, implementer, local community, and individual user. To analyze the trends and extract considerations that could be integrated for implementing digital ID systems in the future, four key relationships between these stakeholders and their impact on digital ID systems were evaluated.

1. **Government to implementing organizations,** to examine mechanisms that need to be in place to ensure the delivery of services using digital ID systems including legal enabling environment to ensure reliable regulations and infrastructure.

2. **Individual to implementer/service provider,** to understand the trust processes required to facilitate the efficacy of these programs to capture the implementer's best practices and from the user perspective.

3. **Service provider to service provider,** to examine interoperability between different systems.

4. **Individual with community,** to understand community cryptocurrency and trust mechanisms, and how can these be integrated or extrapolated to other programs.

GOVERNMENTS TO IMPLEMENTERS

SERVICE PROVIDERS TO INDIVIDUALS

SERVICE PROVIDERS TO SERVICE PROVIDERS

COMMUNITY TO INDIVIDUAL

A combination of online literature, expert interviews, and end user interviews contributed to the synthesis of information presented in the report.

State of the art: Desk research targeted recent (<5 years old) peer-reviewed publications, white papers, and case studies of digital ID use in humanitarian settings, which were reviewed and synthesized for trends. These findings were supplemented with information from high-level design workshops in Nairobi, Kenya led by our partner organizations (Norweigian Refugee Council (NRC), Norwegian Church Aid (NCA), Save the Children Norway, Norwegian Red Cross, and Innovation Norway).

Expert interviews: The first round of interviews comprised of experts in the sector, as identified by the Engineering for Change expert network. Interviews were conducted with representatives from the following organizations: NRC (Norwegian Refugee Council), Caribou Digital, Compulynx, Branch International, Sarafu, Bamba Chakula, Grassroots economics, GSM Association (GSMA), Cash Learning Partnership (CaLP), International Rescue Committee (IRC), ID2020, Omidyar Network, Harvard University, Jomo Kenyatta University of Agriculture and Technology, World Vision, MasterCard

and Mercy Corps; among others. Interview participants were recruited via email and 60-minute semi-structured interviews were conducted via video-chat software.

Technology selection: After synthesizing online and expert viewpoints, a list of leading digital financial tools with embedded digital ID systems in East Africa was generated (full list available in Appendix 1). From this list, seven prominent solutions were selected for detailed analysis (Table 1) to understand practices in the authentication process and the integration of digital ID into the selected services. Selection criteria was two-fold: (1) solutions represented breadth of user provision models, based on the four key stakeholder relationships previously described and (2) solutions had relatively high adoption and usage rates in Kenya.

Practitioner interviews: Once technology solutions were identified, representatives from these companies, such as employees and directors, were recruited for another round of interviews. Semi-structured interviews were held over the phone to gain insights to each technology, stakeholder interaction level, as well as general field insights.

User interviews: To include the end user perspective, 13 Kenyans participated in semi-structured in-person interviews with an E4C Kenyan research fellow. Of the individuals interviewed, six used Sarafu currency and seven used Branch International. The age of participants ranged from 23 to 56 (average = 31) and gender was fairly balanced. Participants' occupations varied, including students, business-persons, and teachers; among others.

Findings: Cooperation Across Digital ID Actors

Various stakeholders play important roles in the service and implementation of digital ID solutions. Notably, across current digital solutions, outlined in Table 1, SIM cards remain the most common factor, illustrating the importance of telcos. In all the digital ID solutions, telcos play the role as the "authenticator" of the ID of the users, via SIM card access.

Table 1. Selected Digital ID technologies in East Africa.

Perspective	Solution	Implementing organization	Description & Sector	Registration process			Payment process		
				Email/ social media	ID number	In person	SIM card (m-money)	Restricted SIM	Bank account
Gov - Implementer	Bamba Chakula	World Food Programme	Humanitarian initiative for cash/ voucher transfer for undocumented populations.			**X**		**X**	
Individual - Service provider	Kionect	Mastercard	Digital log of transaction data that qualifies small business owners for loans		**X**	**X**	**X**		
	2KUZE	Mastercard	Platform connecting small scale farmers with buyers		**X**	**X**	**X**		
	Mastercard inclusive digital identity	Mastercard	Innovative biometric hashing and artificial intelligence technology for safe enrollment and authentication		**X**		**X**		
Individual - Service provider	Branch Intl.	Branch International	Financial access to credit via an app	**X**			**X**		
	PesaPal	PesaPal	Multiple options for online payment	**X**			**X**		**X**
Individual - Community	Sarafu Credit	Grassroots Economics	Community cryptocurrency for an inclusive financial ecosystem			**X**	**X***		

*Users were not required to have individual SIM cards, rather, an agent used a single phone to provide service to an entire community.

Findings: Part 1
Government to Implementers

An Identity document (ID) must be recognized by governments or multilateral organizations, which is why the enabling regulatory environment for digital ID technologies are vital. Otherwise these digital ID solutions could only be used for data management and cash transactions. To improve efforts, NGOs and multilaterals should coordinate and advocate for enabling regulatory environments.

Governments also should understand the importance of adapting present regulations in identity documentation and ICT legal framework to improve quality of life and economic prosperity. For example, Mastercard Labs For Financial Inclusion chose to launch their first project, the Mastercard Farmers Network (MFN), in Tanzania instead of Kenya given regulations on interoperability and mobile money.[1]

Regulations must have a strong focus to improve users' access to resources, rather than simple restrictions on transfers. Some examples of mechanism that could be used to influence decision makers at the government level to adjust ID regulations to benefit the end users of humanitarian crises include:

> **Refugees in Uganda:** In Uganda, refugee documentation is recognized universally and can be used for cash transfer, as a temporary travel document, and to register a SIM card. This was partly due to unrestricted advocacy in Uganda where mobile network operators were lobbied to provide coverage to the Bidi Bidi refugee camp in the northern region. This business case was built through a de-risking program developed by GSMA and funded by the UNHCR and UNCDF, where mobile operators would be reimbursed for the development of a mobile tower if they did not earn a profit [32]. Mobile operators were then incentivized to provide coverage in areas that might typically be overlooked or regarded as not generating enough revenue to be worth the investment.[2]
>
> **Natural disaster in the Philippines:** In 2014, Oxfam and Visa developed a new partnership to advance financial inclusion to people affected by a natural disaster (Typhoon Haiyan) in the Philippines. Aid recipients would receive a prepaid cash card which was initially only valid for Oxfam, but then the regulator (the Central Bank) was lobbied by local cash working groups to reduce KYC requirements and accept that ID at the banks [9].

Furthermore, held in Johannesburg, South Africa, the ID4Africa event highlighted the importance of individual identity for development and reaching the Sustainable Development Goals (SDGs) in African nations. Participants pointed out that although feasible technology already exists, "political will is part of the problem". The role of the private sector to lead innovation was also mentioned. Omidyar network sponsored the event with the goal to ensure all identification related developments in Africa follow the "Good ID principles" [10]. Further, GSMA is exploring regulatory and policy trends impacting digital identity, and particularly the role of mobile technology [6, 11].

[1] Interview with Nzau Muinde, Mastercard Labs For Financial Inclusion, MFN

[2] Interview with Jenny Casswell, GSMA

Findings: Part 2
Service Providers to Individuals

It is essential that the design of the digital ID solution take into account the specific user context, which includes understanding their literacy rates, current notion of identity, trust in local authority, and cultural preferences; among others. Thus, digital ID solutions cannot be quickly replicated from one region to another, rather, they must be specifically designed for the unique set of users considering local context. Importantly, convenience, trust, and consent are essential attributes for digital ID systems:

Convenience: Implementing organizations should particularly focus on designing a service that is convenient and meets users' daily needs. Findings from interviews with Kenyan users of Sarafu-Credit and Branch International determined that individuals are more likely to define trust in terms of convenience, including attributes of safety, speed, and flexibility. Assessing the local understanding and preferences of "convenience" (e.g. ease of access to service/cash, ease of access to customer service, etc.) is essential. Specifically in Kenya, users do not mind registering for multiple SIM cards as long as the services are convenient to access (i.e. the services do not require extensive time or money). However, programs that require travel out of town to collect cash or other services are considered inconvenient and can be a financial burden for users. Often, communities choose a representative who travels to the next city with 10-20 prepaid cards and PINs and collects money on their neighbors' behalf. However, if there are any issues with travel, the representatives may take a 'commission' from community members, jeopardizing trust. Thus, incorporating convenient and trustworthy systems into design of digital services is essential.

Trust: Although user-perceived convenience outweighed perceived trust, mechanism for maintaining user trust is essential for project success. In Kenya, trust processes mainly stem from users' interactions and trust of local agents, providers, and government entities, rather than the specific technology itself. The local providers were more likely to understand the context and build localized trust with a long-term track record within the community. Several interviewees discussed the importance of spending significant time within the given community, which increases trust and the ability to design a context-appropriate solution. An additional attribute of trust, which is context-specific, is ID familiarity. Implementers should be aware of users' customs and perceptions of various forms of ID since some groups may be fearful or unaccustomed to the concept of digital money. For example, when given ATM cards and mobile money registration, some displaced people immediately redeem their allowance as a form of self-security.[3] Understanding of local user priorities and concerns, sufficient inclusion of training programs, and available field support staff can improve user trust in a digital ID solution.

Consent: Consent was a recurring theme from the implementers' perspective rather than the user perspective. In the field of development, service providers are responsible for incorporating a robust and authentic model for individual consent to ensure that all users of the service understand and agree to the terms and conditions.

[3] Interview with Lili Mohiddin, NRC

Findings: Part 3

Service Provider to Service Provider

Partnerships between service providers are essential for successful implementation of robust digital ID systems. Trust, data security, and interoperability are key attributes for giving users a quality service.

Trust and partnerships: Service providers should maintain trustworthy brands, particularly to users and their partners. This trust is based on expertise, availability, scalability, and presence in their locations of service. For large-scale digital implementations, such as digital ID programs, partnerships are key to ensuring quality service. Choice of partnerships allows organizations to combine access to infrastructure, users, and other resources. It should be noted that within the humanitarian sector, partnering with organizations with shared values and incentives will greatly streamline the service and partnership.

Telco influence: Overall, telcos play a central role in digital ID solutions in East Africa, particularly regarding data sharing agreements, privacy, regulation, and ultimately, control over mobile cash transfer. The point of entry of all the solutions that were analyzed and most solutions in East Africa are the SIM cards, thus they become an embedded ID authenticator. Telcos have a financial incentive to become involved in digital ID, and are vital to ensuring success. However, it should be recognized that telcos are for-profit businesses with incentives to focus their services towards higher-income urban populations, which may contradict the needs of humanitarian organizations aiming to implement solutions for rural and/or displaced populations.

Data security, privacy, and transparency: Service providers should clarify which parties own the data, how are databases managed, maintained, and information access rights and limitations. Providers should be aware that national policy may not account for all privacy and security measures and therefore they should implement their own privacy policies to ensure safe practices with their users.

The security of personal data must be considered in any digital ID implementation. Multi-level partnerships with governments, multilateral organizations, and the private sector each have varying levels of associated risk. Suitable standards, agreements, and enforcement of data security procedures are vital to ensure user protection. Digital ID systems have the potential to provide government access to large quantities of personal data, which could have unintended consequences, such as using data to influence elections or monitoring certain demographics. Furthermore, partnerships with the private sector create a higher risk environment for data privacy and protection as there is often less regulation than with government partnerships. For example, Equity Bank in Kenya was discovered using beneficiary data for direct marketing, since there is no current policy or contractual obligation to protect these data.[4] On the other hand, Mastercard stores data for its financial inclusion platforms in East Africa at US data centers with PCI (Payment Card Industry Data Security Standard) compliance in place, to ensure that their users are not targeted by external groups.[5] On the MFN platform specifically, farmers give consent prior to registering for the platform and own their data. MFN service providers, such as international development organizations or banks, have access to aggregated de-identified data, but not individual attribute data or personal details.

[4] Interview with Evelyn Aero, NRC

[5] Interview with Edwin Kaduki, Mastercard Labs For Financial Inclusion

For rural or refugee populations, these risks of personal data breaches from private sector and public sector are much higher since these individuals are often further removed from information flows and may not be aware that their personal information is being compromised. Thus, partnerships with telcos and other actors, and the mechanisms in place to protect user data, should be carefully considered at every stage of a digital ID implementation.

Issues of unintended consequences, such as data breaches, also raise concerns regarding organizational responsibility and accountability. A clearer delineation and physical record of responsibilities for all actors involved in a digital ID service could increase accountability and reduce data misuse. Furthermore, concerns of data privacy rise when reputable organizations, such as the UNHCR or WFP, share information and data with third parties and technology providers [12, 13]. Sharing user data, particularly those of marginalized and vulnerable groups, with third parties is extremely controversial.

Interoperability: In the context of digital ID systems, interoperability is defined as the exchange of personal and systematic identity information between different organizations to reduce the duplication of effort (e.g., user registration process). When considering interoperability, providers should be mindful that exchanging information does not necessarily translate to efficiency gains, which ultimately depend on pre-agreed agreements and clear understanding of roles. A fair data exchange system can be very beneficial, for example when smaller NGOs partner with larger groups, such as the UNHCR and WFP, to capitalize on larger databases and existing digital ecosystems. However, partnerships between small and large NGOs may include unbalanced power relationships, wherein smaller NGOs often provide much of the on-the-ground support but lose control over data and decision-making.

On the organizational side, a significant obstacle to increased interoperability is the lack of policy, data sharing agreements, and the presence of competition or misaligned goals between organizations.[6] Efficiency in the backend of digital systems depends on pre-agreed agreements and a clear understanding of roles between partners, particularly when there are finite resources within organizations. Achieving interoperability requires organizations to agree on standards at multiple levels and leverage technology to meet these standards—not just on technical data formatting but also operational processes, legal agreements, and governance mechanisms.

Despite several challenges with interoperability, there are benefits that might increase efficiency and optimize limited human and technological resources. Some initiatives to promote interoperable systems include the Collaborative Cash Delivery Network[7] which is a group of 15 international NGOs (including Mercy Corps, NRC, Oxfam, and others) that established a partnership to deliver cash effectively and at scale. The goal is to facilitate programmatic and operational interoperability between agencies and standardize contracting and 'backend' systems. Humanitarian programs often rely on partnership-based databases, particularly those used by a larger agency such as UNHCR or WFP. However, this is much less common for smaller NGOs due to scaling difficulties. Another attempt to improve organizational interoperability includes Caribou Digital's 2018 recommendation to establish a multi-stakeholder working group on interoperability, ideally chaired by the UNHCR [11]. The goal of this group would be to agree on a set of standards for technical interoperability such as APIs, data integration, and exchange. The efficacy of a similar system should however be carefully weighed with the inevitable risks and complexities to be faced.

[6] Digital ID Kenya High-level design Workshop, May 27-29 2019, Nairobi

[7] Collaborative Cash Delivery Network webpage: https://www.collaborativecash.org/

Findings: Part 4

Community to Individual

Ultimately, end users want a quality service that meets their needs, is convenient to use, and operated by locally-accessible agents.

Convenience: Everyday users (i.e. those not in disaster/relief settings) recurrently mentioned that they valued the convenience of financial inclusion apps over trust. In these cases, adequate access points and support services should be provided and the ease of accessing services should be evaluated.

Local operators: Trust in the field operators was paramount to a successful operation. A local, or someone who has been a part of the community for a long time and speaks the language, is needed to establish user trust and adoption of services. One way Grassroots Economics provided both an improved service to their clients, while also gaining their trust, was through partnerships with local cooperatives, such as a local maize mill. These partnerships offer collateral for local currencies, which act as vouchers for user goods and services. Additionally, local agents and field operators required by Know Your Customer (KYC) principles are generally trusted because they are highly familiar with the area and people, and speak the local language. These agents are generally existing M-Pesa[8] agents, who exchange the Community Currency for Kenyan shillings using a special system account. Registration requires only the ownership of a SIM card, and users are able to share phones and M-Pesa accounts, highlighting the trust generated within the community. Users also have a personal account and PIN, so transactions feel private and protected. Grassroots Economics also created paper vouchers in the absence of a digital system.

End user perspective: Ultimately, digital ID solutions must serve the end user, who should always be regarded as an active agent, rather than merely a recipient of aid. Interviews with users of Branch International and Sarafu customers (a product by Grassroots Economics) found that common user concerns included lack of agents for transactions, long waiting periods for transactions to complete, and lack of transparency regarding conversion rates of Sarafu points to case.

[8] M-Pesa is Kenya's leading mobile money platform, operated by Vodafone and Safaricom, Ltd.

Additional Digital ID Trends

Digital interventions must be disseminated in enabling environments that allow the services to operate efficiently and ethically. Trends that enable successful digital ID solutions include (1) trust, (2) standards and policy, and (3) ICT infrastructure; in addition to overarching global initiatives and collaborations.

Trend 1: Trust

In the design and deployment of digital ID systems, practitioners in the field must incorporate trust-building mechanisms at all levels. Interorganizational trust is key for building partnerships, and is influenced by two main factors:[9]

1) A long-lasting relationship with the 'front face' of the service (e.g. the local distributor in the case of Kionect and Farmers Produce Organization for Mastercard Farmers Network), and

2) Strong and reliable brand names, such as Unilever (distributor), KCB (Kenya Commercial Bank) and Mastercard.

To provide a digital ID service, trustworthy partnerships are essential. Partnership selection depends on the brand, expertise, availability, scalability, and presence in target locations. The choice of partners is often determined by the way in which the program is implemented in the field and first mile access, and generally necessitates prior contextual analysis. When forming partnerships, humanitarian agencies often seek out service providers who share the same values, whereas local private actors may be more inclined to take a profit-driven approach. When a project is funded by an external donor, this relationship must also be taken into account since solutions must comply with donor requirements and priorities.

The success of the initiative also relies on beneficiary trust in the implementing organization. For example, the success of the mobile money service M-Pesa in Kenya relies partly on the trust that customers have in Safaricom [14], one of Kenya's most well-respected private companies that organizes a large network of M-Pesa agents. Investing in communication and informing users about organization, the data collection process, and the information systems supporting the service can serve as trust mechanisms. In the refugee context, trust factors can be addressed during the registration process by ensuring that users have given informed consent to the collection and storage of their personal data. Furthermore, trust builds on the persistence of field staff who work directly with users.

Country-specific legal frameworks and policies play a significant role in privacy and data protection, which ultimately affect user trust. Users are generally less comfortable with sharing their biometric or any digital data with organizations or governments that lack data trustworthy policies or standards.

Trend 2: Standards and policy

While mobile platforms can help verify and authenticate digital IDs, privacy and data protection are essential to building trust with end users [15]. Standards can improve the accountability and transparency of services by requiring providers to define and articulate the terms of their service and disclose who the data is being shared with. Standards can also be designed to encourage providers to implement simpler solutions that minimize the amount of personal data collected to achieve the service provider's outcomes. In addition to how data is collected and shared, standards and/or checklists should outline how the data will be authenticated, stored, and secured. Furthermore, multi-level stakeholder agreement and partnership upon a set of standards is needed to enable cooperation, increased efficiency, and data privacy.

These agreements will ultimately depend on existing local and national government policies and regulations, which are context dependent. The World Bank has published a recent report on selecting appropriate technology and data standards, which also includes initial 'checks' for building interoperability frameworks [16]. Notably, among their list of

[9] Interview with Jemima Kariuki, Mastercard Labs For Financial Inclusion, Kionect

'checks' is identifying localized legal barriers to interoperability, such as geographic restrictions on data storage and restrictions on technology use. Advocating for changes in regulatory environment usually comes from an organization's country level offices and coordinating efforts among multiple NGOs can create a more efficient and streamlined process to advocate for regulatory change. However this approach still faces challenges since NGOs and multilateral organizations have different operational practices and various relationships with local governments.

Consent: Organizations implementing digital ID systems must be intentional regarding their models for individual consent, which must go beyond 'box-ticking' and include a careful explanation of important terms and conditions.[10] Forced consent, where users are not given a true option to opt-out of data sharing because they need the services offered through having the ID, should be imperatively avoided. Forced consent becomes a problem especially when it requires sensitive data points in addition to name and address, such as biometrics. Clear definitions, openly accessible information, descriptions of what will happen to users' data, and alternate solutions are needed so users can have freedom of choice to make a fully informed decision regarding their options. Holding information campaigns and then conducting a follow-up survey to evaluate their effectiveness can be a starting point. However, if the ID service is the only option for individuals to access government or financial services, users have little choice but to use the system. For this reason, several sources, including Omidyar Network, suggest that digital IDs should not be mandated [17]. In India in 2018, the court ruled that that the previously mandatory national ID system was no longer compulsory for citizens after private companies began purchasing personal data from the local government in Aadhaar [18].

Biometrics: Including biometrical data into a digital ID platform poses some risks that must be proactively mitigated, such as arbitrary, illegal, or unauthorized access and data sharing, individual covert surveillance, data selling, cyberattacks, and political manipulation [19]. A report by The Engine Room and Oxfam regarding the use of biometrics in the humanitarian sector, concluded that the potential risks of incorporating biometrics in refugee services are very likely to outweigh potential benefits [20]. Furthermore, Kenyan civil society activists recently blocked the collection of biometrics for a government HIV study, concerned that data could be misused [21]. Special considerations and recommendations for the use of biometric data include avoiding centralization, ensuring that providing biometric identifiers is voluntary, minimizing data collection and transfers, and ensuring the security of scanning devices and development of legal procedures and standards [22]. A report from Paysafe emphasizes that transparency is the best tool to build trust and that users should be informed about security processes [24, 25].

Trend 3: ICT infrastructure

A digital ID solution must be designed for its intended context of use, which may consist of low or no connectivity and/or no power supply [24]. Consideration of national, local, and individual access to ICT infrastructure is required:

1. National: Availability of reliable service providers, telecommunication infrastructure, regulations and national policy.
2. Local: Region-specific connectivity.
3. Individual: Availability of mobile devices and consideration of users who share mobile phones among friends and/or family.

Telcos and other smaller telecommunication service providers are considered the "middle men" in most of the solutions available in East Africa. These telcos essentially act as the "authenticator" of the ID systems since SIM cards are the initial marker of inclusion. Thus, relationship with telcos and their services, should be included in the implementation strategy early on.

[10] Interview with Aiden Slavin, ID2020

Global Trends for the Future

As technology continues to progress and digital solutions are increasingly integrated into society, future trends include increased partnerships and corporations, as well as an idealized concept of self-sovereign identity.

Consortia: The establishment of consortia such as ID2020,[11] ID4D[12] and Decentralized Identity Foundation[13] confirms the relevance of collaborative efforts towards digital ID solutions. The Sovereign Identity for All (I4A) Council, which published a list of guiding principles [25], aims to develop a more inclusive and ethical identification systems. The World Bank-led ID4D consortium released several case studies, including a Technology Landscape for Digital Identification [26]. ID4D also recently released a draft practitioner guide outlining best practices and considerations for ID systems in developing contexts [16]. The evolving document addresses both technology and data standards, and includes a technical standards decision tree that guides a choice in standard to follow based on the technology employed. Additionally, Good ID[14] is a movement focused on user control, data protection, and trust in the design of digital ID systems. Good ID's best practices include individual control, transparency, use of ethical frameworks, open standards and open source technology to reduce dependency on one single vendor, and prioritizing trust [17]. The organization also specifies that systems should include design features such as privacy, inclusion, user value, user control, and digital security.

Self-sovereign identity: Self-sovereign identity (also known as human-centric data) is a movement recognizing that an individual should own and control their identity without the intervention of administrative authorities [27]. This process adheres to the principles of transparency, consent, interoperability, and portability; among others. The driving concept is that users can store their digital ID data on their own devices and that there is no centralized data storage. This decentralized identity model relies on distributed ledgers (e.g. blockchains) and requires supporting network infrastructure and high levels of digital literacy, which may represent a challenge in many contexts. Sovrin's report on the use of distributed ledger technologies in the humanitarian sector includes two case studies in identification management which can serve as examples of increasing identity owners' sovereignty [28]. Although a promising concept, most implementations are only in pilot stage [29].

[11] ID2020 webpage: https://id2020.org/
[12] ID4D webpage: https://id4d.worldbank.org/
[13] DIF Identity Foundation webpage: https://identity.foundation/
[14] Good ID webpage: https://www.good-id.org/en/

Conclusion: Defining a Context-Specific User Provision Model

While providing an enabling environment is essential for successful implementation of a digital ID system, a strong contextual analysis regarding a digital ID system's user provision model is mandatory. Given the complexity of digital ID systems, solutions should not be replicated without considering the context-dependent variables. These context dependent variables include the user needs, preferences, local usage of technology, trust in identification systems and sociocultural structural conditions. Notably, local user support services, such as information help desks and reliable local staff, should be integrated.

Furthermore, depending on the model, end users of digital ID systems may not be the beneficiaries but rather implementers, service providers, or local government. While the users of digital ID systems may receive access to services and assistance, there may not be economic incentives to specifically incorporate their needs and preferences into the design of the solution. Thus, designers should intentionally consider the needs and conditions of all users and stakeholders of the system.

Understanding users, preferences, and structural conditions: To implement any digital solution, thorough understanding of the users' context, preferences, and structural conditions is essential. A community-based approach that incorporates direct user engagement to examine various factors (e.g. low digital literacy levels, difficult geographical access, social structures and preferred communication networks, etc.) to evaluate the suitability of proposed technological solutions, sets of standards, necessary partnerships, and implementation strategy. Implementing co-design processes and user-led design strategies is essential to delivering a successful intervention. Along these same lines, designers must consider that their technologies will be embedded into existing socio-economic structures that inherently include status quo and social inequities. Among important factors, gender-inclusive structures and frameworks are essential [30]. A study examining the ability of mobile phones to empower women in Bangladesh found that they merely perpetuated the existing gender stereotypes and had the potential to even further undermine gender equity [31]. Similar issues could arise with the use of mobile technologies for digital ID, especially when women are already disproportionately affected by a lack of ID.

Inclusive provision models: The World Bank emphasizes the importance of inclusion and the fact that no one should be denied access to digital ID services due to a lack of connectivity or technical skills [1]. However, UNHCR data show that low digital literacy levels among some user groups create a barrier to the use of Internet and ICT services [8]. According to Caribou Digital [11], it is critical that efforts towards increasing access pay attention to individual user needs, particularly the need to strengthen their control over the use of their personal data. Therefore it is essential to design inclusive provision models for ID systems and services.

User support services: Convenience and trust build on the persistence of field staff that facilitate relationships on the ground. While it is critical to place staff near end users (e.g. local help desk), humanitarian organizations may be short staffed and lack region-specific language and cultural skills. To overcome this barrier, some NGOs hire local representatives or partner with local organizations to fulfill first mile duties. Regardless of the method, solutions must include reliable and convenient support services for users who encounter questions or concerns.

Thinking Ahead: A Checklist for Implementing Digital IDs

Ultimately, the goal of implementers is to improve the lives of populations in situations of vulnerability, who require access to services and local resources. With this in mind, a solution must be context-specific and appropriate, digital or not. To evaluate the user provision model, a table of considerations that includes trust, convenience, standards, data security, interoperability is provided.

Designing an appropriate user provision model is of utmost importance, given that solutions cannot be directly replicated across contexts. To guide practitioners, the checklist presented below provides a guideline for important considerations for digital ID implementation.

Question	Resulting Considerations
1. Define the needs of the project, outlining: a. What services will be provided? b. What is the provider needed for? (e.g. data authentication, collection, storage, exchange/transmission) c. Who is the end user? d. What is the end user looking for in an ID-based service? What are their priorities and concerns?	**Interoperability.** Depending on what service the technology provider is needed for, interoperability may/may not be required. It decided on a case by case basis. **Defining end user.** If digital ID is being exchanged or stored, then the end user may be the implementing organization, rather than an individual user. In this case, there should be extra emphasis on defining the relationship between implementer, government, and IT provider to establish roles and trust processes.
2. Define the characteristics/needs of the end user and setting. If the end user is a person in a situation of vulnerability, this would include, but is not limited to: a. Digital literacy rates b. Gender/gender norms c. Access/infrastructure d. Analysis of trust and convenience	**Consent.** If digital literacy rates are low, consent needs to include a training program. Users should be presented with multiple options, which is the responsibility of the implementing organization to provide. **Inclusive provision.** If there are gender inequities, the distribution of technologies and services may be affected. **Technology used.** If there is a lack of connectivity, consider paper-based ID, or creating partnerships with local telcos to develop the infrastructure. **User value.** Depending on the context, users may value trust (high-risk, vulnerable settings) or convenience (everyday user) more, influencing marketing strategies. **Access/support services.** If convenience is a main concern, define access points and support services, and measure ease of obtaining services. **Local agents.** If trust is a main concern, invest in local agents who have spent a long time and are well known in the community.
3. Define the regulatory environment on the local, regional, and national level.	**Standards.** Data and technology standards will be influenced by the prevailing regulations.

	Data interoperability regulations. The project may/may not require additional considerations for data interoperability regulations like data protection laws, counterterrorism normative, etc. These requirements will depend on project goals and partners. **Data collection/storage.** Depending on the regulations, certain systems may not be accepted and therefore cannot be used (e.g. SIM card for refugee contexts). **Cross-sectoral regulations.** Understand the legal limitations of refugees within their new country to ensure the digital solution complies.
4. Define the partnerships needed, including: a. Public/private partnerships b. Governments to implementing organizations	**Regulatory changes.** Advocate for regulatory changes that enable access to services and facilitate public/private partnerships. In some cases, the creation of public/private partnerships could drive governmental changes and new legislations to adapt to new challenges. **Telcos partnerships**. In East Africa, specifically in Kenya, the definition of the needs and partnerships with telecommunication provider is required early on in the project, since they are usually the middleman and play a very important role in the services provision (All the solutions selected use SIM cards as a payment method. See Table 1)

References

[1] World Bank Group. Principles on Identification for Sustainable Development: Toward the Digital Age, February 2017

[2] Bouma, Tim. Public Sector Profile of the Pan-Canadian Trust Framework Version 1.0, July 2019

[3] United Nations. Sustainable Development Goal 16, Accessed on October 2019

[4] Digital ID Kenya High-level Design Workshop, presentation by Gravity Earth, July 2019

[5] Gelb, Alan; Clark, Julia. Identification for Development: The Biometrics Revolution. Center for Global Development: Working Paper 315, January 2013.

[6] Theodorou, Yiannis; Okong'o, Ken; Yongo, Erdoo. Access to Mobile Services and Proof of Identity 2019: Assessing the impact on digital and financial inclusion. GSMA, 2019.

[7] GSMA, Refugees and Identity: Considerations for mobile-enabled registration and aid delivery. GSMA, 2017.

[8] UNHCR. Country Reports: Displaced and Disconnected. UNHCR & GSMA, 2019.

[9] Bright, Jake. Mastercard launches 2KUZE agtech platform in East Africa. Tech Crunch. January 2017.

[10] Hersey, Frank. Omidyar Network hopes to ensure African digital ID is 'Good ID'. BiometricUpdate.com. July 2019.

[11] Schoemaker, Emrys; Currion, Paul; Pon, Bryan. Identity at the margins: Identification systems for refugees. Caribou Digital. 2018

[12] Kaurin, Dragana. Data Protection and Digital Agency for Refugees. World Refugee Council Research Paper No. 12. May 2019

[13] Raymond, Nathaniel; McDonald, Laura Walker; Chandran, Rahul. Opinion: The WFP and Palantir controversy should be a wake-up call for humanitarian community. Devex. February 2019.

[14] Mas, Ignacio; Morawczynski, Olga. Designing Mobile Money Services: Lessons from M-PESA. *Innovations.* Spring 2009.

[15] Basis Research, The role of privacy frameworks in building trust for digital identity services, GSMA, 2019.

[16] World Bank Group. Identification for Development Practitioner's Guide. Version 1.0. October 2019.

[17] Omidyar Network. Omidyar Network Unpacks Good ID. May 2019.

[18] Mozilla. Aadhaar: Key challenges and a way forward. Accessed in October 2019.

[19] Carmona, Magdalena Sepúlveda. Is biometric technology in social protection programmes illegal or arbitrary? An analysis of privacy and data protection. ESS-Working Paper No. 59. Social Protection Department, International Labour Organization. 2018.

[20] The Engine Room. Biometrics in the Humanitarian Sector. Oxfam. 2018.

[21] Davis, Sara L.M; Maleche, Allan. "Everyone Said No": Key Populations and Biometrics in Kenya. Health and Human Rights Journal. July 2018.

[22] National Digital Identity Programmes: What's Next? Access Now Policy Paper. May 2018.

[23] Capps, Robert. The Biometric Trust. BiometricUpdate.com. June 2019.

[24] UNHCR. Connecting Refugees: How Internet and Mobile Connectivity can Improve Refugee Well-Being and Transform Humanitarian Action. September 2016.

[25] Sovrin Foundation. Sovrin Identity for All Council Charter-Version 2. March 2019.

[26] Bachenheimer, Dan; et al. Technology Landscape for Digital Identification (English). World Bank Group. February 2018.

[27] Sovrin Foundation. What is self-sovereign identity? December 2018.

[28] Slavin, Aiden. Distributed ledger identification systems in the humanitarian sector. Sovrin Foundation. May 2019.

[29] International Federation of Red Cross and Red Crescent Societies. Learning Review: Blockchain Open Loop Cash Transfer Pilot Project. September 2018.

[30] GSMA. Exploring the Gender Gap in Identification: Policy Insights from 10 Countries. April 2019.

[31] Sultana, Sharifa; Guimbretière, François; Sengers, Phoebe; Dell, Nicola. Design Within a Patriarchal Society: Opportunities and Challenges in Designing for Rural Women in Bangladesh. *Proceedings of the 2018 CHI Conference on Human Factors in Computing Systems*, April 21-26, 2018, Montreal, QC, Canada.

[32] GSMA. Humanitarian Payment Digitisation: Focus on Uganda's Bidi Bidi Refugee Settlement. GSMA. 2017

Appendix 1: Current Digital ID Solutions

Presented is a table with several examples of technological solutions for digital ID, elements of success, and lessons learned.

East African Digital ID Solutions (part 1/3)

Name	Type	Success	Lessons Learned
M-PESA	Mobile money (Kenya) Private sector	Success relies partly on the trust that customers have in Safaricom, one of Kenya's most well-respected private companies, and a large network of M-PESA agents. Other success factors are ease of registration and simple and transparent pricing.	Failed in other countries, e.g, South Africa due to a lack of partnership between telecom and banking sector.[15]
Aadhaar	National ID (India) Government	1.2 billion people or 99% of India's population has a digital proof of identity.	Lack of privacy and transparency. Mismanagement of biometric data.
Huduma number	National ID (Kenya) Government	Still in implementation phase	Criticized for mandatory registration and poor governance did not fully consent.[16]
Gravity Earth	Self-Sovereign ID, vendor/ private sector company based in Kenya	Allows users to have control over their data. The solution highlights the importance of portability of verifiable credentials in refugee contexts.	Assumption that each user has a smartphone and constant connectivity is often not realistic in a refugee context.
YOTI	Portable encrypted NFC-enabled tag (Private sector)	Designed for use without a smartphone or an official ID document. It was specifically designed as a digital identity solution in humanitarian context, in areas with little or no connectivity. Yoti claims to follow the ethical principles for biometrics.[17]	Still in pilot phase

[15] Mbele, Lerato. Why M-Pesa failed in South Africa. BBC Africa Business Report. May 2016.
[16] Bomu, Grace. Policy concerns with digital ID in Kenya. Research ICT Africa. June 2019.
[17] Dawson, Julie. Yoti supports the seven ethical principles for biometrics. Yoti. April 2019.

East African Digital ID Solutions (part 2/3)

Name	Type	Success	Lessons Learned
Bamba Chakula	Cash/voucher mobile transfer (Kenya) NGO-private partnership, Allowing financial inclusion of undocumented populations	Bamba Chakula is the most cost efficient cash delivery mechanism WFP has used so far. Users prefer mobile money because it gives them a perception of safety compared to cash. It was very successfully implemented in refugee camps in Kenya in 2015. The system incorporated the following features to ensure that it gained special approval from the Communications Authority:[18] ● The SIM cards have restricted functionality and can only be used to receive the electronic vouchers, and not for telecommunication services. ● Humanitarian agencies took responsibility for customer identification and verification: WFP and UNHCR work together to validate eligible beneficiaries and distribute the SIM cards. Safaricom as the telecommunication service provider does not engage directly with individual refugees or have sight of their personal details. ● Harmonized Databases: Data sharing agreements between organizations ● Safaricom provides SurePay solution, a closed loop payment system for electronic vouchers.	WFP's recent announcement of partnership with the Silicon Valley-based big data analytics company Palantir sparked criticism as it involved sharing user data with a third party.[19]
Kionect	Platform for small business owners	The partnership with Kaskazi, a for-profit wholesaler and distributor, and Diamond Trust Bank (DTB), a financial institution with operations in Kenya, Uganda, Tanzania and Burundi, is facilitating digital payments between the kiosk owners and the wholesaler, and is also acting as a re-seller of the platform to its wholesale business clients. Kionect technology provides a digital log of transaction data that qualifies these micro-retailers for loans to stock inventory from Musoni, a regional microfinance provider. With every loan that is paid on time, the kiosk	Pilot

[18] GSMA, Refugees and Identity: Considerations for mobile-enabled registration and aid delivery. GSMA, 2017.

[19] Raymond, Nathaniel; McDonald, Laura Walker; Chandran, Rahul. Opinion: The WFP and Palantir controversy should be a wake-up call for humanitarian community. Devex. February 2019.

		owner has the opportunity to take out a larger loan for a longer term and further contribute to the growth of their business.	

East African Digital ID Solutions (part 3/3)

Name	Type	Success	Lessons Learned
2KUZE	Platform for small scale farmers	2KUZE gives farmers access to more buyers, enables them to run a more profitable business and paves the way to a cashless agricultural sector. Through a grant from the Bill & Melinda Gates Foundation, the Mastercard Lab for Financial Inclusion is working with East African entrepreneurs, governments and other stakeholders to develop local products rooted in the company's global knowhow.	Pilot
Branch International	Microfinance	It offers a fast and convenient way to access credit via an app. In Kenya, the mobile loan is sent through user's mobile money (M-PESA) or bank account. Users can build up their credit limit every time they repay a loan. The company recently partnered up with VISA.	Although registration is possible with email/ social media account, a SIM card (end therefore a national ID) is required for payment
Pesapal	Online payments	Pesapal partners with banks, mobile network operators and credit card companies to give consumers as many payment options as possible. Available payment options are M-PESA, Airtel money, and credit/debit cards.	Relies on mobile money, which requires a national ID
Mastercard inclusive identity	Digital inclusion	Innovative biometric hashing and artificial intelligence technology for safe enrollment and authentication	Pilot