Migrant Money

Portable Digital Identification as an Enabler to International Remittances

ACKNOWLEDGEMENTS

On behalf of the migrant women and men originating from, and receiving remittances in, and their wider communities in the least developed countries, the UNCDF Migration and Remittances programme team would like to thank the many partners and collaborators who are contributing to our efforts to advance low-value remittances flowing seamlessly through cross-border payment systems. This appreciation is not their endorsement of this report and is extended to Bank for International Settlements Innovation Hub (BISIH), Bill and Melinda Gates Foundation, Calp Network, Caribou Digital, Center for Financial Regulation and Inclusion, Stellar Development Foundation, Tony Blair Institute for Global Change, and UNDP.

This report is a result of the successful collaboration between **UNCDF Migration and Remittances Programme**, led by Mamadou Diallo, and **Accenture Development Partnerships** led by Sebastian Rodriguez, with invaluable inputs and support from Sara Puebla (UNCDF), Julie Kamau (UNCDF), Doreen Ahimbisibwe (UNCDF), Jack Keeling (Accenture), Carlotta Abbott (Accenture), and Chui Yan Yau (Accenture). Amil Aneja provided overall guidance and coordination.

The authors would also like to thank John Powell, and Justine De Smet, for editorial and design support.

The UNCDF Migration and Remittances programme has been made possible by the generous funding support from the Swiss Agency for Development and Cooperation (SDC) and from the Swedish International Development Cooperation Agency (Sida). This work is a product of the staff of the UNCDF with external contributions. The findings, interpretations, and conclusions expressed do not necessarily reflect the views of the UNCDF, its executive board and donors, or the governments they represent. UNCDF does not guarantee the accuracy of the data included in this work.

Contents

1. Executive Summary

Digital identity is a key enabler for transactions in our daily lives, helping embed trust in these daily interactions. Some industries put in rigorous identity requirements to underpin and harness this trust, such as Know-Your-Customer (KYC) requirements within the financial services industry. The benefit of providing digital identity to assist citizens in their daily lives can have a huge economic gain, with the potential to unlock 3-13 percent of GDP in 2030 (McKinsey, 2019).[1] Both public and private sector organisations recognise this value, evidenced by the many different digital identity schemes and infrastructures that exist worldwide. However, while digital identity initiatives and solutions are advancing globally, many of these initiatives exist within a single country or are within a small block of countries.

Since there are so few successful cross-border digital identification systems globally, people on the move (migrants) are presented with challenges when accessing critical services such as financial services, including remittances and government services. Often, they are required to show physical credentials multiple times to human agents to prove their identity – an expensive, time-consuming, and potentially impossible process, depending on the state of their physical identities (lost, stolen, left behind in a rush to flee). A lack of global standardized digital identity regulation results in inconsistency among the types of ID individuals possess, and equally inconsistent KYC regulations mean that not all ID documentation is accepted in different countries.

Beyond their importance, remittance payments are key economic drivers as well – by 2030, the remittance market size is projected to reach US$1,227.22 billion by 2030 (Allied Market Research).[2] These financial flows provide crucial support for purchasing essential items such as food, health, and education during periods of economic hardship in migrants' countries of origin. If states could increase the ability and adoption of formal (digital) financial services to be used by migrants for remittances, flows would be more secure, increase at a greater rate, and make more impact (i.e., more money going to people in need). Since identification is one of the core building blocks for end-to-end digitalization of remittances, it is of paramount importance to gain a better understanding of challenges and learnings linked with cross-border and portability of these identification systems. Without this portability, costly and risky remittance payments will continue. The UNCDF considers the portability of ID from the migrant's perspective to ensure migrants' digital IDs are recognized and accepted across borders. This can be achieved through several scenarios, including agreements between governments or regional organizations and/or interoperability through standardization.

The UNCDF conducted this mixed-method research project to understand the state of digital identity globally, why cross-border projects have failed to progress, and what can be done to resolve existing pain points. Through our study, the following global challenges have been identified:

- **The lack of internationally implemented and consistent standards** for KYC and digital identity negatively impacts interoperability across borders.[3]
- **Risk and liability concerns for implementation of a portable digital identity solution** among both governments and financial services providers which leads to reduced adoption of digital identity solutions.
- **Lack of interoperability between existing digital identity system**s due to differences in implementation globally.

1 https://www.mckinsey.com/capabilities/mckinsey-digital/our-insights/digital-identification-a-key-to-inclusive-growth
2 https://www.alliedmarketresearch.com/remittance-market
3 https://www.fatf-gafi.org/en/publications/Financialinclusionandnpoissues/Digital-identity-guidance.html

- **Lack of formal legal identity globally**, which leads to migrants utilizing informal cross-border payment channels with higher risks associated.
- **Lack of regulatory clarity and data protection laws** lead to trust issues over digital identity adoption.
- **Lack of governance model and trust framework** to establish reputation and trust in implementing digital identity programmes.
- **Limited technology accessibility, digital and financial literacy, and cultural barriers** result in challenges in establishing and expanding national ID systems which are secure, workable offline and inclusive.
- **Lack of public and private partnerships** to discuss and drive ecosystem participation and seek economically viable solutions in implementing cross-border digital identity.

Overcoming these challenges would require global collaboration and cooperation toward a common goal and mission. This is the key requirement to see meaningful movement toward portable digital identity. While regional digital identities such as the EU Digital Wallet are beginning to be implemented, the following recommendations can accelerate progress globally:

- Create, facilitate, and maintain conversations with **diverse stakeholders to discuss ecosystem and data governance models** and identify **mutually beneficial opportunities for collaboration**.
- Create **"safe" sandbox environments for data management testing and assurance and revise risk management frameworks** to align with the digital landscape.
- **Increase awareness and improvement of existing industry standards**, confirming understanding of regulation, mutual acceptance and sharing of best practices.
- Increase engagement to **agree on a trust framework for digital identity within financial services** which assists with international standardisation efforts, mutual acceptance and sharing of best practices.
- Invest in and **drive coordinated campaigns on improving digital literacy** and access to education and increase digital inclusion.
- **Strengthening political/commercial bilateral ties** across major migration corridors, i.e., multinational banks that have a physical presence across countries, could play a more proactive role.
- **Identify viable economic corridors** between countries for developing meaningful use cases and improve or expand safe payment corridors with the adoption of digital identity to accelerate cross-border acceptance.
- **Establish interoperability and standards for portable digital identity** by leveraging technologies such as biometrics and the capabilities of digital wallets.

Utilization of these recommendations is key to unlocking the value portable digital identity can bring by harnessing and improving trust, which is critical for successful implementation. Stakeholders, embracing collaboration, can begin to realise the full value of portable digital identity, such as greater access to the growing formal remittances market and promoting greater financial inclusion for all. We hope the research and insights gathered within this report will help advance these conversations and allow those stakeholders to understand what steps are required to bring this vision to life.

2. Introduction

It is estimated that around 850 million people globally lack a form of official identification, something that is required to comply with financial regulations at the point of onboarding to formal financial services (ID4D, 2022).[4] Migrants are particularly likely to not have any official identification or face difficulties in verifying their identity in foreign countries, which may hinder their ability to rely on formal financial service providers to send money across borders. However, even when the money flows through formal channels, costs tend to be highest when sent through banks, with an average cost of 11.84 percent in 2022 (World Bank, 2022).[5] Overall, the cost of sending $200 across international borders averaged 6.4 percent of the amount transferred in the first quarter of 2021, according to the World Bank's Remittance Prices Worldwide Database. This is more than double the United Nations Sustainable Development Goal target of 3 percent, which is set out within goal 10.C (United Nations).[6]

These barriers not only impact migrants and their families but also have direct macroeconomic and social development consequences on low- and middle-income economies. The global remittance inflows were estimated at $831 billion in 2022, with this forecast to increase to $858 billion by 2024 (KNOMAD, 2023).[7] In particular, low- and middle-income countries around the world heavily rely on this source of income to boost their economies. Whilst remittances drive economic growth, challenges remain for many migrants wishing to access formal remittance channels (United Nations).[8] Needless to say while the cost of ID may be high for the migrant workers, the cost of the remittance through formal channels may be linked to other reasons like compliance, trapped liquidity, correspondent banking relationships, etc.

To allow for greater access to formal channels, creating a better solution for the trustworthy identification of individuals is of paramount importance. Often, individuals are required to show physical credentials multiple times to human agents to prove identity – a time-consuming, expensive and potentially impossible process, depending on the presence and state of physical identities (lost, stolen, left behind in a rush to flee or non-existent). Therefore, for people on the move, proving their identity can be a challenge and put them at risk of corruption and extorsions.

4 https://id4d.worldbank.org/global-dataset
5 https://remittanceprices.worldbank.org/sites/default/files/rpw_main_report_and_annex_q422_final.pdf
6 https://www.un.org/sustainabledevelopment/health/#:~:text=Goal%203%20targets,-_3.1%20By%202030&text=3.3%20By%202030%2C%20end%20the,diseases%20and%20other%20communicable%20diseases
7 https://www.knomad.org/publication/migration-and-development-brief-38
8 https://www.un.org/en/desa/much-more-%E2%80%98lifeline%E2%80%99-millions-households-remittances-can-spur-global-growth-says

Figure 1: Definitions of digital identity and portable digital identity

Digital Identity

A collection of individual attributes associated with a uniquely identifiable individual (e.g., name, date of birth, occupation, health status) stored and authenticated in the digital sphere, and which are trusted and used for transactions, interactions, and representations online and in the digital world.

Portable Digital Identity

Portable digital identity enables people on the move to use their digital identity issued in their origin country for authentication purposes across borders.

The concept of digital identity has grown in the last twenty years as the digital world has expanded. The benefits of digital identity can bring huge economic gains, with studies identifying the potential to unlock 3-13 percent of GDP by 2030 (McKinsey, 2019).[9] Both public and private sector organisations recognise this value, and many different digital identity solutions and schemes now exist worldwide.

According to the World Bank, "When IDs issued by one country are recognised by other countries – whether for face-to-face or online transactions – they become a powerful driver of economic and regional integration" (ID4D).[10] Currently, proving one's identity in a foreign country when accessing financial services can be a struggle, even for those who have valid forms of identification. However, a solution that enables the digital identification of citizens, which can be used across borders and even sectors, could unlock value for those migrants who face these issues. Eliminating current acceptance barriers offers significant economic and social advantages, but achieving this poses a worldwide challenge. It necessitates global collaboration and coordinated efforts to establish a trusted identity ecosystem for mutual benefit.

Finally, it's important to acknowledge the necessity of a digital ecosystem for fostering the development of digital IDs. Additionally, it's crucial to acknowledge and plan the continued need for many citizens to hold physical credentials, even as digital IDs are being introduced.

3. Methodology

The purpose of this research study is to explore how the portability of digital identity could be leveraged to improve the access and usage of formal financial services, including digital

9 https://www.mckinsey.com/capabilities/mckinsey-digital/our-insights/digital-identification-a-key-to-inclusive-growth
10 https://id4d.worldbank.org/guide/mutual-recognition-ids-across-borders-0#:~:text=When%20IDs%20issued%20by%20one,promote%20safe%20and%20orderly%20migration

remittances by international migrants. This report has been written following a mixed-method research study comprising a desk-based literature review, interviews with industry experts and a review of case studies. To develop insights on this topic, a research team was formed focusing on the following areas:

- **Foundational ID Landscape** – Understanding the current environment for different countries regarding their foundational ID landscape, adoption, solutions and usage domestically.
- **Client Onboarding** – Understanding how different financial service organisations from different jurisdictions onboard new customers, be those domestic clients or migrants, especially looking at types of identification and channels used.
- **Digital Identity Infrastructure/Adoption/Portability/Standards** – Understanding the different systems and infrastructure in place for digital identity solutions globally, the uptake of such solutions, where they can be used, what standards and best practices they adhere to and portability across borders.
- **Migration and Remittances** – Understanding the different migration and remittance patterns for countries and where the most pertinent corridors exist.
- **Technology Infrastructure** – Understanding a country's digital and technology infrastructure regarding internet usage and outreach, mobile phones and other such advancements.
- **Policy and Regulatory Frameworks** – Understanding the current state of policies and regulatory frameworks concerning financial regulation and digital identity.

To further the understanding gained through desk research, the research team sought the perspectives of a wide selection of experts through Key Informant Interviews (KIIs).

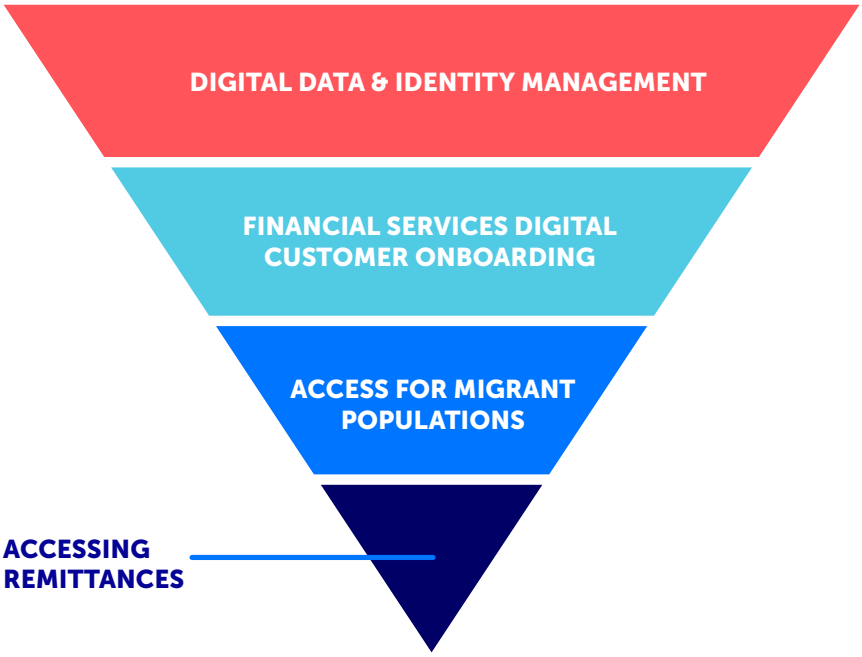
A total of 42 KIIs have been conducted across organizations and independent experts globally. Stakeholders were selected from financial services providers, international remittance service providers operating in many jurisdictions, solution providers, development professionals, and experts from academia and public institutions to glean insights.

After the global desk research and KIIs, four countries were down-selected for further deep-dive as case studies. The four countries (Bangladesh, Colombia, Germany, and Kenya) were selected based on evaluation criteria which considered factors such as:

- **Domestic digital identity Infrastructure** – The level of digital identity within each country was assessed. Those who had successfully produced a digital identity solution or were looking at ways to create a solution in the near future were deemed high in the evaluation.
- **Financial Services Regulatory Frameworks (AML/ KYC/ CFT)** – Countries were required to not be on any Financial Action Task Force watchlists while also adhering to international or regional KYC/AML/CFT regulations.
- **Migration Patterns and Remittance Flows** – Countries that either had large migration and remittances inflow and/or outflows were prioritised, especially when comparing migration to population size and remittances to GDP.
- **Foundational ID Landscape** – Countries were scored on the prevalence and adoption of foundational ID domestically. This was then analysed against similar countries within regions.

Four major categories were established to focus the investigation and categorize the results, analysis, and suggestions. The categorisation below was designed to help understand the approach required for migrants to be able to use digital identity for remittances. First, by understanding the digital data and identity management complexities, then understanding how financial services organizations onboard customers and then, more specifically migrants for the use of sending remittances.

Figure 2: Levels of analysis



Level	Description	Examples
Level 1: Digital Data and Identity Management	Adoption of digital data and identity management solutions and use of digital technologies for customer relationship management	• Data Ownership and Management • Data Security • Digital Transformation
Level 2: Financial Service Onboarding	Adoption of digital identity technologies for the Financial Services industry and the customer onboarding journey	• Financial Services Regulation • Liability and Trust Frameworks • Customer Experience
Level 3: Access for Migrant Populations	Digital onboarding journey for migrant populations wishing to access Financial Services.	• International/Cross-Border Context • Availability of Foundational IDs • Political/Cultural/Social Differences
Level 4: Accessing Remittances	Migrants wishing to send or receive remittances rather than any other financial products.	• Consumer Preferences and Habits • Cost of Sending/Receiving • Formal vs Informal Remittances

4. Benefits of Digital Identity

While identification has been traditionally conducted using paper credentials, processes are now increasingly incorporating digital technologies. Digital technologies bring great promise as they are cheaper, more easily portable than physical documents, and could improve ease of access or, indeed, enable new access for individuals who have traditionally been unable or unwilling to use formal financial services. Particularly in developing economies, a multi-purpose digital identity has become a critical tool for not only uniquely identifying citizens but also supporting the social and financial inclusion of underserved and vulnerable communities (IISD, 2022).[11] The United Nations Sustainable Development Goals recognise the importance of identity and provide the target that all people will be able to obtain a "legal identity" by 2030 (SDG 16.9), given approximately 850million people are still unable to prove who they are (United Nations) (Identification for development, 2022).[12] [13]

4.1 Benefits For Migrants

Providing legal identification to those in need. The surge in digital identification technologies seems to meet a pressing need that could be especially beneficial for migrants, who may be particularly vulnerable to a lack of legal recognition and social exclusion. For migrants who may not be in familiar territory, this ease of access may enable services to be provided online and across borders which otherwise could not be reached. For example, in Estonia, once migrants are enrolled in the national identification system, they have the option to apply for a digital ID, which allows them to access different e-services and gives them equal access to e-services as citizens, improving their quality of life (UN Refugee Agency, 2021).[14]

A key advantage of an accessible digital ID for migrants is the security of the person from exploitation as well as unreasonable, unlawful or protracted detention by authorities. When a person loses their identity by merely crossing borders, it puts them in a very vulnerable position, even despite having a physical credential. The vulnerability is exploited by human traffickers as well as exploitive labour practices. Similarly, people can be subject to prolonged, unreasonable, or unlawful detention by authorities and exploited through prison systems if their identity cannot readily be ascertained. Digital IDs that link to physical identifiers are critical in these scenarios to enable vulnerable people pathways to dignity.

Greater access to services and unlocking existing barriers to entry. Portable digital identity can enable individuals to not have to authenticate their identity face-to-face, resolving possible communication, travel, and logistical barriers that some migrants might face when moving to another country. It also helps to broaden access to financial services to individuals who may be from more vulnerable demographics who may have additional needs and could particularly benefit from the use of digital channels, including women, the elderly and the disabled. (Joseph Rowntree Foundation, 2008).[15] As one of the remittance providers stressed, digital identity enables individuals to "*not have to move around and meet face-to-face*", making services easier and broadening access to certain groups of individuals, such as women or those with disabilities. For example, they may be confined within secluded accommodations or workplaces far from remittance access points and agents, or they might not have the identity or residency documents required for making or receiving money transfers. Meanwhile, banks

11 https://sdg.iisd.org/commentary/generation-2030/leveraging-digital-identity-for-greater-financial-and-social-inclusion/
12 https://www.unodc.org/roseap/en/sustainable-development-goals.html#:~:text=Target%2016.9%20%2D%20By%202030%2C%20provide,national%20legislation%20and%20international%20agreements.
13 https://id4d.worldbank.org/global-dataset
14 https://www.unhcr.org/neu/70493-unhcr-strengthens-efforts-on-digital-identity-for-refugees-with-estonian-support.html
15 https://www.jrf.org.uk/sites/default/files/jrf/migrated/files/2234.pdf

and other remittance service providers (RSPs) may not recognise low-skilled migrant women as an important customer segment, as they tend to transmit smaller amounts.[16] Financial service providers (FSPs) may also inadvertently exclude many women migrants through poorly designed know-your-customer (KYC) or due diligence processes.

The benefits of digital IDs also extend to overcoming the challenges of damaged physical IDs. Replacing ID cards can come at a large personal expense or inconvenience. Digital IDs solve the common problem of people choosing not to replace their IDs even if they become severely damaged (and therefore unusable), in effect placing them in the population without IDs. Moving to digital removes the risks and burdens of keeping a physical ID intact.

4.2 Benefits For Financial Service Providers

Improved financial crime risk management. One hundred percent of interview respondents said they believe that Digital Identities can improve financial crime risk management. Reasons cited often included the benefits that digital identity could bring for data management both internally within organisations and externally within the wider industry. Many of the current challenges in effective risk management and compliance are due to a lack of data, so improving data availability of quality and reliable data from an independent, trusted source was perceived to be a good outcome from a risk management and compliance perspective (FATF, 2023).[17] Additionally, data standardisation with respect to the data attributes held for customers on customer profiles that are currently inconsistently gathered via disparate KYC processes was considered to bring greater efficiencies for internal processing and also associated reductions in cost to operations. There is a degree of standardisation that a digital process can mandate and enforce that manual procedures cannot reach (given human errors and inevitable gaps and flaws in manual processing), which was also seen to be favourable when addressing digital identity adoption.

Digital identity can help bring greater customer context than exists currently in traditional forms of ID. Given there's so much more information that a digital identity could provide about a customer, and especially if that digital identity is used for multiple purposes across several industries, financial service providers could have far more context as to who their customers are than simply completing a tick-box exercise of gathering a handful of data points. Some respondents stated that they believed (digital identity) would enable better integration of the customer ID with the wider customer account information. Also, there is increasing use of technology such as machine learning algorithms and artificial intelligence for ongoing customer monitoring (FATF, 2013).[18] The more closely account information can be linked to individual customer IDs, the better, as it enables financial service providers to have a greater understanding of individuals, especially as the ID can accumulate data over time. Better and more up-to-date customer profiles, with greater context, mean more accurate risk assessments, better decision-making, and fewer instances of unintended financial exclusion (FATF, 2013).[19] Taken together, more standardisation in digital identity, greater efficiency and more easily being able to do entity resolution to increase assurance that a customer is who they say they are, is overall considered highly beneficial.

16 UNCDF 2024, Remittances Gender Synthesis Report.
17 https://www.fatf-gafi.org/media/fatf/documents/recommendations/pdfs/Guidance-on-Digital-Identity-Executive-Summary.pdf
18 https://www.fatf-gafi.org/content/dam/fatf-gafi/guidance/Opportunities-Challenges-of-New-Technologies-for-AML-CFT.pdf.coredownload.pdf
19 https://www.fatf-gafi.org/content/dam/fatf-gafi/guidance/Opportunities-Challenges-of-New-Technologies-for-AML-CFT.pdf.coredownload.pdf

Entity Resolution: Entity Resolution is a technique to identify data records in a single data source or across multiple data sources that refer to the same real-world entity and to link the records together.

Consistent usage of digital identity information throughout the payment chain and operations is advantageous for both organisations and individuals. Not only could customer KYC processes be enhanced, but also the wider set of operational and compliance activities required by regulations (that can negatively impact a customer experience) can be streamlined and made more efficient, opening opportunities for underserved populations to access financial services and increase financial inclusion. Transaction monitoring, payments screening and screening for Sanctions, Politically Exposed Persons (PEPs) or Negative News could also all be greatly improved through the widespread adoption of Digital ID. Today, these have been very problematic areas for Banks that must grapple with cross-checking imperfect identity information with multiple datasets that create vast swathes of false positives and lead to huge operational costs, delays in processing payments, poor customer experience and hours of time and effort in the back-office to discount risk and resolve false positive alerts. If digital identity and payments can be linked up, as intended in the EU's e-IDAS 2.0 regulation, which looks to combine digital identity with a digital wallet, this could minimise data processing errors upstream, enable more automatic screening in real-time, and could benefit both organisations and customers (Council of EU, 2022).[20] Financial services providers interviewed believed that the ability to place an identity to every payment in their system is very powerful and can help them understand money flows. The projected total cost of financial crime compliance across financial institutions worldwide in 2022 was $274.1 billion, up from $213.9 billion in 2020 (LexisNexis, 2023).[21] If done well, Digital ID could reduce some of this operational cost through increased processing efficiencies.

e-IDAS 2.0 Regulation: In 2021, the EU Commission published on 3 June 2021 a legislative proposal that updated their previous e-IDAS regulation to enable EU citizens to prove their identity and share electronic documents from their "European digital identity Wallets" (European Parliament, 2022).[22]

Trusted digital identities have the potential to be at least as trusted, if not even more reliable, than traditional identity forms and potentially reduce impersonation fraud. While the world is more familiar with physical IDs (which may then be linked to online government records), these can be easily manipulated or purchased illegally (Forbes, 2021).[23] If there is trust in the tool and the source, some interviewees believed Digital IDs could be safer than receiving, for example, certified paper copies of traditional documents. Although many parties use certified paper copies, it is not often that there is a process step to confirm that that notary or the lawyer who's allegedly signed the documentation exists, an obstacle that is especially challenging in a cross-border context.

20 https://www.consilium.europa.eu/en/press/press-releases/2022/12/06/european-digital-identity-eid-council-adopts-its-position-on-a-new-regulation-for-a-digital-wallet-at-eu-level/
21 https://risk.lexisnexis.com/global/en/insights-resources/research/true-cost-of-financial-crime-compliance-study-global-report
22 https://www.europarl.europa.eu/RegData/etudes/BRIE/2022/699491/EPRS_BRI(2022)699491_EN.pdf
23 https://www.forbes.com/sites/jumio/2021/05/03/how-national-digital-ids-benefit-both-citizens-and-businesses/

Enhanced ability to reach the un-banked or under-banked customer base and increase the number of migrants and their families opting for formal remittance channels. The major attraction of informal remittance channels, such as hawala systems, are their characteristics of having lower costs, faster speeds, and no control framework. If digital identity enables greater cost efficiencies and faster transfers while ameliorating trust and financial crime risk management, a wider range of customers may be enabled to use formal financial services who would otherwise have been excluded by the fact that the risk management was too expensive for them to be commercially viable. If financial service providers create new infrastructure using digital identity, they could, therefore, save money and create new and potentially very lucrative revenue streams. This could entice a wider range of customers to the formal sector but also allow better macro risk management across the financial services industry.

4.3 Benefits for governments and Policy Makers

Support greater enablement of government services, facilitating citizens to participate in the broader digital economy. In many instances, lack of identification leads to struggles for individuals in securing basic government services, including access to public healthcare, education, voting services and financial programmes. A digital identity will make these services more accessible while improving quality of life. Creating reliable and more comprehensive datasets improves the ability to deliver targeted public services with more context as to who the receivers are whilst also enabling wider societal benefits for communities such as avoiding corruption, siphoning off resources, double counting, minimising tax evasion and targeting errors in beneficiaries, and reduces costs and bureaucracy related to physical documents. Digital identity can catalyse the improvement of a country's fiscal capacity by being instrumental in promoting financial inclusion and growth of the formal economy by designing for inclusive and flexible requirements while ensuring that enrolment points are accessible to all segments of the population.

Enhanced security for citizens and government departments/operations: Digital identity systems can strengthen security measures by providing a secure and reliable way to authenticate individuals. Strong authentication mechanisms, such as biometrics or multifactor authentication, can be incorporated into digital identity solutions which can further reduce the risk of identity theft, fraud, and unauthorized access to sensitive information. However, governments must address privacy and data protection concerns (decentralized digital ID schemes can help in this), promote harmonized legal measures on this topic, and enable equitable access for all citizens. Digital identity is a public good, and governments should ensure that solutions meet the needs of all their citizens without excluding any.

4.4 Benefits for the NGO's and Development Sector

Digital identity solutions can facilitate the registration or enrolment process in the humanitarian sector which in turn allows for better provision of support and services to those who need them. Digital platforms are restructuring how companies and industries operate, including NGOs and humanitarian organisations operating in the development sector. These entities operate in complex environments and serve vulnerable populations, including people on the move, often with incomplete information or imperfect resources. Indeed, not only could digital identities increase access for everyone, but they could also potentially increase access for individuals who do not have any form of foundational ID at all. Humanitarian organisations can assist governments in providing foundational IDs to their beneficiaries who do not have an officially recognised form of ID, and they can also provide a form of scalable, functional ID that can, over time, accrue a transaction history and, with it, cultivate a higher degree of trust with service providers.

Digital identification technologies do indeed show promise for extending humanitarian

services to new beneficiaries and enhancing existing services to current beneficiaries. Digital infrastructures are playing an increasingly prominent role in the lives of the growing number of people on the move around the world (Wiley Online Library, 2021).[24] Empowerment passes through digital inclusion: access to jobs, income and remittances, online learning and web-based economic activities will make a difference in the lives of people on the move. Equally, a number of large international NGOs are looking at using digital identity to help deliver secure payments, acknowledging that they can no longer complete their operations with a spreadsheet and beneficiary ID cards. Additionally, many of the fraud and trust issues NGOs face when delivering cash-based programming or cash vouchers can be further eliminated by a trusted, secure digital identity solution. Helping them better coordinate and streamline support to beneficiaries, making the whole system more effective and efficient. However, despite their promise, digital identity solutions require careful planning and consideration to ensure their suitability and efficacy and cater for local requirements and conditions.

Finally, a secure digital identity system has the potential to unlock increased donor funds for NGOs. Donor due diligence on NGOs includes understanding the NGO's end recipient compliance programmes, including screening and verification. This is especially true for NGOs with direct cash transfer and voucher programmes. A higher identity standard could help increase donor confidence in the destination of their funds.

5. Cross-border Digital Identity Implementations and Implications

Within our research, we looked at digital identity maturity globally and the existence of cross-border identity and digital identity implementations. This, coupled with analysis and insights from key informant interviews with a range of stakeholders, has resulted in an understanding of the challenges inhibiting cross-border digital identity acceptance. Challenges have been identified at the global level, but also at the regional and national levels for the four country use cases. Though the main challenges are political, there are quite a few regulatory and technological hurdles to solve, pending the political will in both developed and developing countries.

Level 1: Digital Data and Identity Management

Stakeholders are uncertain about the data governance model (ownership, usage, sharing, privacy, compliance, etc.). With many different digital identity implementations worldwide, there are many different approaches to how to provide this solution to citizens. One of the key aspects of these solutions is how individuals' personally identifiable information is stored, used, and shared to ensure organizations receive the correct assurances that the individual wishing to access the services is validated. However, while these data governance models exist for domestic digital identity solutions, there remain questions about how they work for cross-border initiatives. Respondents believed that several different regulations exist in relation to privacy and storage that do not correlate over different jurisdictions. They highlighted that the lack of interoperability in the governance of data internationally means countries will face difficulties in allowing its use across borders, challenges that will require collaboration and cooperation to ensure interoperability.

Changing security and fraud risks need to be considered prior to adoption, e.g., from individual risks to dataset-wide breaches. Many financial service institutions interviewed still have reservations about accepting digital identity as opposed to the usual identity verification

24 https://onlinelibrary.wiley.com/doi/full/10.1111/isj.12353

and proofing methods they currently use. Due to risks associated with using digital identity technologies (especially those which have not been implemented by governments) and the implications of allowing bad actors through their systems, organizations' risk levels remain high when onboarding individuals, especially migrants.

Market competition vs collaboration creates siloed solutions with incompatible designs and technologies. Many digital identity solutions today currently sit within siloes meaning that individuals can only use them at one organization. Governments, NGOs, and financial services organizations interviewed believed this means that organizations compete against each other to enable individuals to use digital identity and face uncertainty about allowing others to utilize it. This has led to various incompatible designs and technologies internationally, which means individuals are unable to use digital identities in their own ecosystems, making it difficult to ensure different solutions are compatible once adopted.

Different data regulation approaches exist that make it difficult for identity to be accepted internationally. In recent years, nations such as China, the United States, the EU, and the Middle East have devised their own strategies for safeguarding the data privacy of their respective citizens. While data privacy holds paramount significance in the contemporary era of technology, the absence of consistency in international data privacy regulations presents challenges when understanding how digital identity can be used across borders, as the storage, use, processing, and acceptance may have different implications dependant on where the identity has been issued versus where it is being used.

Digital identity is not fully realised or given to all citizens globally. A fundamental reason that prohibits digital identity across borders is that countries may not have robust national digital identity solutions. According to respondents, in order to kick off such an initiative, countries planning a cross-border digital ID project must first have each national digital identity that is currently used in the financial sector for onboarding before understanding how to accept other digital identities for such a process.

Level 2: Financial Service Onboarding

The lack of internationally implemented and consistent standards for KYC and digital ID adds complexity to the design and leads to a lack of interoperability between solutions. Each country or region has its own unique set of rules and protocols for customer identification, making it challenging for multinational companies to establish a uniform and efficient system. The differences in KYC standards mean that a digital identity may be used for onboarding in one country while it is not accepted in another. In addition, digital identity has few recognised standards internationally, which further creates siloes by allowing different interpretations in terms of use, technology, approach, and others.

Regulatory pre-approval is a pre-requisite for adoption but creates a first-mover deterrent and free-rider benefits. Before organizations can accept digital identity, this must be first regulated and embedded in law to ensure its proper use and safeguarding. However, not only does this regulation often require a huge uplift to ensure it works for all parties, but it also creates deterrents to being the first movers within the market to accept digital identities. Respondents believed that organizations were fearful of the risks associated with introducing the technology before it's being proven in the market.

Perceived increases in liability or risk exposure can require lengthy multi-party acceptance or cause paralysis. With digital identity ecosystems, there is a large benefit for the individual to be able to use their credentials wherever they wish in daily life. However, with such systems, some issues become apparent when understanding who owns the liability of the credentials.

When interviewing financial services companies, it became apparent that in such a high-risk industry, many felt uncomfortable relying on the checks completed by other organizations or governments to trust the attestations being made.

Political/cultural/social differences internationally inhibit a standardised or one-size-fits-all approach. As already suggested, many digital identity solutions around the world differ in various ways. For example, the Aadhaar system in India is a biometric digital identity issued by the government to enable individuals to identify themselves for both the public and private sectors (UIDAI).[25] However, in Sweden, digital identity is issued to individuals by financial institutions through BankID (BankID).[26] In addition, the success of digital identity also differs greatly due to different cultural, political and social factors such as digital literacy and trust within government and also technology. This has led to a myriad of different approaches to digital identity that make it difficult for a one-size-fits-all approach which would enable greater use across borders.

Lack of technology infrastructure and access to online services prevents individuals from accessing digital services. Research from the study suggests that countries that have greater technology infrastructure have successful digital identity systems or are currently developing systems to support the growing digital services landscape. A country requires a minimum level of technology infrastructure and digital services to invest in creating digital identity solutions that are useful and valuable to citizens. The business case must become more apparent and create more digital identities for individuals that are used frequently to get countries to accept digital identities from other countries.

Level 3: Access for Migrant Populations

Migrants may have no form of foundational/acceptable ID and may be unable to obtain a new ID. Eight hundred and fifty million people globally do not have any form of official identity documentation (World Bank, 2023).[27] Even for those that have them, they often get lost, forgotten, destroyed or even stolen as people move through borders. For the financial services sector, understanding the identity of individuals is of paramount importance to enable KYC and AML regulations to be satisfied but also to ensure they are aware of those using their services. With so many people lacking even rudimentary and physical identity documentation, the prospect of having a digital identity seems a long way away. Without this basic requirement being satisfied, having digital identity accepted across borders will become increasingly challenging. Financial services providers sometimes insert assumptions from their own context onto identity standards for migrants (ex-address printed on the ID card, reference of the ID limited to numbers, etc.), furthering issues migrants face when attempting to open accounts.

Digital literacy is progressing globally even though access divides exist and create barriers to entry. In our KIIs and research, many believed that there are still large gaps in digital literacy which creates further barriers for digital identity to be used universally. Citizens will only use what they are comfortable with and what they trust, meaning that they often would rather use physical credentials if available. While there are many developed countries with high levels of digital literacy, the gap needs to be closed to make it possible for digital identity to become a useful tool across borders.

The perception that foreigners pose more risk than nationals leads to additional requirements or enhanced due diligence for migrants. When speaking to financial institutions and governments, there was a consensus that migrants pose a greater risk than country nationals.

25 https://uidai.gov.in/en/
26 https://www.bankid.com/
27 https://blogs.worldbank.org/digital-development/850-million-people-globally-dont-have-id-why-matters-and-what-we-can-do-about

While this is not always the case, migrants usually must complete additional requirements or enhanced due diligence when onboarding to accounts to ensure that the risk appetite is satisfied. While digital identity could assist in enhancing efficiencies within this process, there still needs to be further requirements for some individuals, which will lower the user experience and lead many to utilize other financial services and remittance options.

Communication challenges (e.g., language barriers) complicate migrant interactions. For some migrants, language differences create a huge barrier to accessing financial or digital services. Respondents stated that these differences not only made it more difficult for migrants to gain access to financial institutions in the countries where they wanted to work but also drove them to use more "unofficial" channels to move money across borders.

Level 4: Accessing Remittances

Trust, cost, convenience, speed, habit, and reputation hugely influence consumer product selection behaviours and may make informal channels appear more appealing. While digital identity will help create a safer system for organizations, many factors go into the choice of remittances for migrants. Informal remittance channels may appear more appealing to consumers in certain contexts because they can excel in these areas, offering a familiar, cost-effective, and trustworthy way to send money, especially in regions with limited access to formal financial services.

Informal remittances prosper across major migration corridors. In major migration corridors, there is a high likelihood of close-knit migrant communities. People within these communities often have strong trust and personal connections with one another. Other factors may be more advantageous to some migrants, such as the opportunity for reduced expenses and the ability to avoid the banking infrastructure. Respondents believed that some individuals may have ulterior motives for keeping themselves out of regulated services, something that would lead many to utilize informal channels.

5.1 Africa

Cross-border Initiatives	Countries Affected	Objective	Description	Status	Enablers	Challenges
Smart Africa Trust Framework – Smart Africa Trust Alliance (SATA) (Smart Africa, 2020)[28]	African Union (55 Member States) Pilot in Benin, Ghana, Senegal and Togo	To establish institutional ownership and accountability combined with a trust framework based on standards and trust assurance mechanisms to facilitate cross-border interactions	To establish a trust framework based on standards and trust assurance mechanisms for digital identity to facilitate cross-border interactions Pilot to help people access services across borders, such as obtaining SIM cards (often requiring ID verification)	In Development (2020) Pilot (2023)	• Allow African citizens to participate in the digital economy • Regional integration in support of The African Continental Free Trade Area (AfCFTA) by enabling a trusted flow of data across borders • Ensure inclusion, security, privacy and data ownership in digital identity systems • Support interoperability and neutrality of digital ID systems	• A large number of people in Africa have no legal means of identification (542 million people in Africa) • Lack of confidence in African national and regional cooperation • Wide disparities between different regulatory frameworks • Only 29 African countries (55 percent) have a specific privacy and data protection law
Inter-State Pass: Mutual Recognition of National IDs (Identification for development)[29]	Kenya, Rwanda and Uganda	Movement of People	Citizens are FREE to move between these countries with only a national ID card	Live (2014)	• Accessible travel for cross-border access to services or trade • Incentivized regularized free movement through formal channels, increasing safety (e.g., women traders) and customs collections	• The verification process is largely manual at borders • Seeking ways to digitalize the processes and to expand it to other interested EAC partner States
East African Community (**EAC**) – **Biometric e-passport** (Envoy Global, 2023)[30]	Burundi, DR. Congo, Kenya, Rwanda, South Sudan, Tanzania, Uganda	Movement of People, Security protecting against identity fraud	New E-Systems aimed at improving efficiency, removing loopholes and enhancing security a move	Live (2022 – Kenya)	• Remove identity verification barriers to conducting business across borders • Include additional security and technology measures that will protect against falsification and identity theft	• High cost of printing new e-passports and phasing out old-generation passports • Except for Kenya, other EAC Member States are at different levels of preparedness

28 https://smartafrica.org/wp-content/uploads/2020/12/BLUEPRINT-SMART-AFRICA-ALLIANCE-–-DIGITAL-IDENTITY-LayoutY.pdf
29 https://id4d.worldbank.org/guide/mutual-recognition-ids-across-borders-0
30 https://resources.envoyglobal.com/global-news-alerts/kenya-introduction-of-biometric-e-passport/

Cross-border Initiatives	Countries Affected	Objective	Description	Status	Enablers	Challenges
Economic Community of West African States (**ECOWAS**) – **Biometric Card** (Biometric update, 2015)[31]	15 Member States Ghana, Senegal and Guinea Bissau issued	Movement of People, Migration data exchange	To harmonize its third-party visa regime, follow similar ones to establish biometric ID cards for all citizens of Africa's largest sub-regional grouping for travel purposes	Live (2016)	• Building foundational ID (fID) systems that are interoperable will have substantial socioeconomic benefits at both the regional and national levels • Achieve its vision of freedom of movement • A collaborative approach among ECOWAS Member States based on common standards	• 53 percent (196 million) of the population of the ECOWAS region are unregistered and do not have proof of identification • Legal and institutional frameworks across Member States tend to be weak and fragmented • Inadequate national ID systems greatly hinder access to services
WURI Program* – Unique Identity Number (World Bank, 2020)[32] (AFDB, 2023)[33]	Benin, Burkina Faso, Côte d'Ivoire, Guinea, Niger and Togo	Facilitate financial inclusion and support service delivery in the ECOWAS community	Looking to create national digital identity systems in 6 West African Countries and enable interoperability between them	In development (2018 – Phase 1 2020 – Phase 2)	• Ensure sustainability for the fID system and robust legal and institutional enabling framework with a regional approach • Allow for e-KYC across the sub-region • Address the main barriers to opening a bank account or obtaining a SIM card with greater financial and digital access and inclusion	• Coverage of national IDs and birth registration remains low, and access to services is greatly hindered • Risks of exclusion and marginalization • Political economy challenges of security or surveillance • High cybersecurity risk when the data are in a "virtual space"
Bank ID System in West African Monetary Zone (WAMZ) (AFDB, 2023)[34]	Gambia, Guinea, Liberia and Sierra Leone	Enhance financial sector efficiency, financial inclusion and regional integration.	The establishment of a digitally interoperable unique bank identification system and harmonised customer identification framework	Funding Approved (Nov 2022) – *Project to begin in July 2023 until June 2026*	• Enhance financial sector efficiency within the participating countries • Increase access to finance • Regional integration in the West African Monetary Zone • Improve KYC, combat fraud, discourage loan defaulting	• Efforts required to link bank accounts to biometric BVN • Potential illiteracy and poor awareness about the process, especially in rural places and among uneducated people • Potential lack of public awareness of the need to link their bank accounts during implementation

31 https://www.biometricupdate.com/201512/distribution-of-ecowas-biometric-id-cards-to-begin-in-january-2016
32 https://documents1.worldbank.org/curated/en/261151588384951057/pdf/Benin-Burkina-Faso-Togo-and-Niger-Second-Phase-of-West-Africa-Unique-Identification-for-Regional-Integration-and-Inclusion-WURI-Project.pdf
33 https://www.afdb.org/en/news-and-events/press-releases/west-african-monetary-institute-receive-8-million-african-development-fund-support-enhanced-banking-identification-and-financial-sector-efficiency-west-african-monetary-zone-6030
34 https://www.afdb.org/en/documents/multinational-west-african-monetary-institute-wamz-unique-bank-identification-ubi-and-digital-interoperability-project-appraisal-report

In the African region, countries have a low to medium level of maturity in the digital identity systems, even if we see considerable government appetite to expand or create national systems in countries including Ethiopia, Kenya, Côte d'Ivoire, Rwanda, Nigeria and Uganda. Growth in digital identity is also spreading in Africa, with regional blocs endeavouring to recognise each other's identification documents to facilitate financial inclusion, free movement of people and cross-border digital trade.

A large number of African citizens have no legal means of identification, leading to a situation where about 542 million people in Africa do not have a foundational identification and, therefore, are considered "invisible" (African Union).[35] Smart Africa, a commitment from African Heads of State and government, supports the African Union's vision to transform Africa into a single digital market through the development of digital identity interoperability and data interoperability designed by the Smart Africa Trust Alliance (SATA) (Smart Africa, 2020).[36] The alliance, in 2020, developed a data exchange trust framework based on standards and trust assurance mechanisms to facilitate cross-border interactions. The approach of the SATA trust framework ties in closely with the work put forward by UNECA's Pan-African Trust Framework, e-IDAS guidance, and the work advancing from the Smart Africa Data Protection Working Group (Smart Africa, 2020).[37] Cross-border integration will require confidence in African national and regional cooperation to ensure the establishment of standard-based digital identity systems. In 2023, as the building block for cross-border digital ID, cross-border Mobile SIM card registration was identified as the first use case for the initial implementation of the Data Interoperability Platform (SATA-DIP) (Biometric update, 2022).[38]

The West Africa Unique Identification for Regional Integration and Inclusion (WURI) Programme, launched by ECOWAS and the World Bank, synergises with the Smart Africa initiative. WURI Programme aims to help improve access to services, including financial and digital inclusion, by financing the development of digital foundational identification (fID) systems in 6 West African countries and enabling interoperability between them (International Telecommunication Union, 2021).[39] In Phase 1 (2018 – 2024), Côte d'Ivoire and Guinea benefited from the funding to develop foundational identification systems that are inclusive of all persons.) (Relief Web, 2023).[40]Considerations were raised during phase 1 implementation, including low coverage of national IDs and birth registration, which hindered access to services, exclusion and marginalisation, as well as diminished people's digital privacy and control over their data due to political economy challenges of fID system for security or surveillance purposes not for service delivery. In Phase 2 (2020 – 2026), Benin, Burkina Faso, Togo and Niger were funded to implement foundational identification systems independently and according to their needs, using a minimal set of attributes to uniquely describe an individual (Relief Web, 2023).[41] To ensure the sustainability of fID systems, promoting mutual recognition of regional fID credentials is the key to the programme. For example, leveraging robust ECOWAS-wide interoperable fID systems to allow for e-KYC across the sub-region brings additional benefits of cross-border trade and labour market integration to the countries (WorldBank, 2020).[42] This is critical in driving financial inclusion and cross-border digital trade, especially for migrants.

In African countries, providing fID to individuals is emphasised in various initiatives mentioned

35 https://au.int/sites/default/files/documents/38507-doc-dts-english.pdf
36 https://smartafrica.org/wp-content/uploads/2020/12/BLUEPRINT-SMART-AFRICA-ALLIANCE-–-DIGITAL-IDENTITY-LayoutY.pdf
37 https://smartafrica.org/wp-content/uploads/2020/12/BLUEPRINT-SMART-AFRICA-ALLIANCE-–-DIGITAL-IDENTITY-LayoutY.pdf
38 https://www.biometricupdate.com/202202/id4d-report-2022-to-see-significant-progress-toward-paradigm-shift-in-digital-id
39 https://documents1.worldbank.org/curated/en/261151588384951057/pdf/Benin-Burkina-Faso-Togo-and-Niger-Second-Phase-of-West-Africa-Unique-Identification-for-Regional-Integration-and-Inclusion-WURI-Project.pdf
40 https://reliefweb.int/report/burkina-faso/togo-benin-burkina-faso-and-niger-join-west-africa-regional-identification
41 https://reliefweb.int/report/burkina-faso/togo-benin-burkina-faso-and-niger-join-west-africa-regional-identification
42 https://documents1.worldbank.org/curated/en/261151588384951057/pdf/Benin-Burkina-Faso-Togo-and-Niger-Second-Phase-of-West-Africa-Unique-Identification-for-Regional-Integration-and-Inclusion-WURI-Project.pdf

above, paving the way to financial inclusion. fID systems, in turn, drive cross-border trade through the free movement of people. In Kenya, Rwanda and Uganda, citizens have been able to travel between these three countries using their national ID instead of a passport after obtaining the inter-state pass at the border control. This has made travel more accessible for those who depend on frequent trips across the border for access to services or livelihoods, yet the verification process of the inter-state pass is largely manual without leveraging digital identity systems in each of the countries (World Bank, 2017) (Smart Africa, 2020).[43] [44] Countries are seeking ways to digitalise the processes and hoping to expand it to other interested East African Community (EAC) partner States. The Economic Community of West African States (ECOWAS)'s National Biometric ID Card is another example of encouraging the free movement of people in the region by replacing residential permits and removing the need to use visas (Biometric update, 2015).[45] The biometric card is currently deployed in Ghana, Senegal and Guinea Bissau, adhering to the Framework of the ECOWAS-European Union Project (ECOWAS).[46] This mutual acceptance of national IDs is mainly purposed for travel, while the verification of identity for client onboarding in financial services is still based on physical checks.

Some countries such as Ethiopia, Togo, Guinea, Morocco, and the Philippines are implementing digital fID systems based on open-source technology (MOSIP) with the objective of not relying on closed-loop technologies and reducing the overall cost. Other countries have recently signed MoUs for pilots, such as Sierra Leone, Niger, Uganda, Madagascar, Sri Lanka, and Burkina Faso. MOSIP has interoperability, currently yet implemented in any use case, that enables cross-border operation. The lack of digital identity systems in African countries has been an eminent challenge that some private sector stakeholders have tried to solve such as Mastercard Community Pass that collaborates with the governments to build a functional digital identity infrastructure that is shared across sectors, such as government agencies and banks, and interoperable.

Mastercard started issuing Community Pass biometric smart cards to citizens in African countries in 2021 to provide a biometric digital ID and a digital bank account (Biometric Update, 2021).[47] Community Pass is operational in Mauritania, Uganda, Kenya, Tanzania and Mozambique (Biometric Update, 2023).[48] The Community Pass focuses on connecting marginalised individuals and hard-to-reach places through offline portable digital identities, for instance, meeting people where they are and digitising life transactions such as vaccination. They can biometrically enrol people offline on the edge with a mobile device to build up a digital footprint for the individual. The focus of Community Pass is on the lowest assurance level of digital identity, which is essentially a way to identify the individual and build trust. The team operates in Uganda, Kenya, India, Mauritania, and Zambia, with the same capabilities used across various use cases in health, payments, and agriculture (Mastercard, 2023).[49] To further expand the influence, there needs to be a network of public and private partners to come together to accelerate data compliance for critical services and cross-border use cases.

In Africa, the main challenge is political will. Beyond the political will, the top three challenges for providing digital identity and enabling it across borders are as follows:

43 https://medium.com/world-of-opportunity/opening-doors-how-national-ids-empower-women-cross-border-traders-in-east-africa-8443c98e2aad
44 https://smartafrica.org/wp-content/uploads/2020/12/BLUEPRINT-SMART-AFRICA-ALLIANCE-–-DIGITAL-IDENTITY-LayoutY.pdf
45 https://www.biometricupdate.com/201512/distribution-of-ecowas-biometric-id-cards-to-begin-in-january-2016
46 https://ecowas.int/ecowas-to-conduct-sensitization-on-national-biometric-identity-card-and-the-fight-against-trafficking-in-persons/#:~:text=The%20ENBIC%20which%20will%20improve,Ghana%2C%20Senegal%20and%20Guinea%20Bissau
47 https://www.biometricupdate.com/202109/mastercard-partnership-to-capture-biometrics-of-30-million-africans
48 https://www.biometricupdate.com/202212/mastercard-africa-digital-id-scheme-to-benefit-from-50m-of-dfc-funding-to-its-partners
49 https://www.mastercard.com/content/dam/public/mastercardcom/na/global-site/public-sector/other/humanitarian-community-pass-january2023.pdf

1. **Inadequate technical and identity infrastructure**. Many African citizens have no legal means of identification, leading to a situation where about 542 million people in Africa do not have a foundational identification and, therefore, are considered "invisible". While the idea of foundational identity remains a key problem, there is a lack of technical infrastructure to provide solutions to the masses. The International Telecommunication Union indicates that 2.9 billion people globally remain offline, around 37 percent of the world's population. In Africa in 2021, only 33 percent of the population was using the internet, meaning an estimated 871 million people are not benefitting from digital dividends (DFAT).[50] For digital identity to be useful to citizens, the right infrastructure has first to be built to allow its utility, especially for the financial services sector. Before even considering how digital identity can be used across borders, technological issues need to be addressed to ensure that they are able to give useful solutions to citizens (which can be accepted internationally) and also create the right operations that allow other digital identities to be used. A large portion of respondents believed that this challenge in Africa was of particular concern to success, together with bridging the digital divide in some African countries.

2. **Different policies across the region lead to a lack of interoperability**. As noted above, there are several cross-border ID programmes within Africa. However, only the ones that are currently centred around acceptance of physical ID documents exist, such as the Inter-State Pass and East African Community (EAC) – biometric e-passport. While these exist, there is a lack of successful cross-border digital identity initiatives currently working in the continent. This has led to different countries and governments taking various approaches and policies toward creating such solutions such as Ethiopia, Kenya, Côte d'Ivoire, Rwanda, Nigeria, and Uganda. Each country is digitizing government services, but their legal frameworks are in widely varying states, from inherited colonial laws through modernization and, in some cases, to amendments of newer frameworks to adapt them to the reality of identity systems now in place. However, Smart Africa is looking at the development of digital identity interoperability and data interoperability with the Smart Africa Trust Alliance (SATA) (DFAT).[51] The alliance, in 2020, developed a data exchange trust framework based on standards and trust assurance mechanisms to facilitate cross-border interactions. The approach of the SATA trust framework ties in closely with the work put forward by UNECA's Pan-African Trust Framework, e-IDAS guidance, and the work advancing from the Smart Africa Data Protection Working Group (UK government, 2021).[52] Cross-border integration will require confidence in African national and regional cooperation to ensure the establishment of standard-based digital identity systems.

3. **There remain data privacy and protection issues across the continent**. Globally, protection is a hot topic, with many countries and regions adopting data protection regulations. Africa is no different here, with several African countries with data protection laws in place, including Kenya (MTI).[53] However, despite this, there are growing concerns that in several African countries, government agencies and private entities are collecting and processing personal data without adequate data protection frameworks amidst weak oversight mechanisms and inadequate remedies. Also, mistrust of how citizens' IDs will be used by other countries and strict data sovereignty laws are serious reasons for the lack of ID interoperability. Fourteen countries have signed the African Union Convention on Cybersecurity and Personal Data Protection and only eight countries had ratified it by June 2020 (Government Technology Agency, 2021).[54] This has led many individuals within Africa to be suspicious of government

50 https://www.itu.int/en/ITU-D/Statistics/Documents/facts/FactsFigures2021.pdf
51 https://smartafrica.org/wp-content/uploads/2020/12/BLUEPRINT-SMART-AFRICA-ALLIANCE-–-DIGITAL-IDENTITY-LayoutY.pdf
52 https://smartafrica.org/wp-content/uploads/2020/12/BLUEPRINT-SMART-AFRICA-ALLIANCE-–-DIGITAL-IDENTITY-LayoutY.pdf
53 https://www.odpc.go.ke/dpa-act/
54 https://cipesa.org/2022/01/data-privacy-still-a-neglected-digital-right-in-africa/#:~:text=There%20are%20growing%20concerns%20that,oversight%20mechanisms%20and%20inadequate%20remedies

led digital initiatives, and groups have been lobbying with governments to ensure that personal data in the digital age is protected and privacy-preserving principles are adhered to. With these debates occurring both in a domestic and regional context, they must be solved before digital identity can become a useful tool for the continent's population.

Kenya Use Case

Historically, M-PESA has served as the primary choice for domestic remittance payments in Kenya, with an impressive 96 percent of households relying on it. One of the primary challenges associated with sending international remittances to Kenya has been the cost, which has averaged around 8.45 percent. M-PESA operates as a mobile money solution, requiring customers to initially register at small retailers, often mobile phone stores, where identity verification takes place (MAS, 2022).[55] During the registration process, individuals undergo know-your-customer (KYC) procedures, which involve the collection of personally identifiable information and subsequent verification checks. Once registered, M-PESA users can deposit cash in exchange for electronic money, facilitating the transfer of funds to friends and family within Kenya and, more recently, to other African countries and various money transfer organizations.

In 2019, an amendment to the Registration of Persons Act paved the way for Kenya to establish a National Integrated Identity Management System known as Huduma Namba. The government's objective was to centralize existing identity systems, rendering them interoperable. However, in 2021, the High Court of Kenya ruled the rollout of a nationwide biometric ID scheme illegal due to data privacy concerns.[56]

In 2023, Kenya officially discontinued the Huduma Namba initiative in favour of its new Unique Personal Identifier programme, a new secure digital ID system.[57] This system aims to link all the country's databases and enable secure and seamless access to a wide range of government and private sector services, including KYC procedures.

The main challenge in Kenya was political will. Beyond the political will, the top three challenges for digital identity and cross-border digital identity in Kenya are as follows:

1 **Lack of proper safeguards for the security of personal data**. This is pegged on Kenya's lack of robust security infrastructure to protect sensitive information and maintain data privacy. There are also concerns about the lack of transparency in how the information is being used and the potential for government misuse of collected centralized data without the consent of the citizens as the data subjects. Additionally, the lack of a data privacy approach limits organizations from adopting open standards that would help greater interoperability in future cross-border use cases.

55 https://www.vodafone.com/about-vodafone/what-we-do/consumer-products-and-services/m-pesa
56 https://3news.com/kenya-court-declares-biometric-id-rollout-illegal/
57 https://www.biometricupdate.com/202305/kenya-unveils-details-on-new-digital-id-rollout-india-potential-partner

2 **Lack of private sector collaboration with digital identity**. While the private sector engages with the government on several aspects, there has been a lack of collaboration around digital identity in Kenya. Ultimately, the lack of a digital identity ecosystem or marketplace is something that will continue to have negative effects on the development of digital identities and their ability to port from different countries from one country to another. This requires a multi-stakeholder approach where different players come to the table and have open conversations on how to collaborate and agree on the development of a healthy digital identity ecosystem.

3 **Lack of internet connectivity will always harness adoption**. According to our research and experience, both Kenya's network and technology infrastructures require improvement to provide digital identity solutions. In January 2023, there were 17.86 million internet users in Kenya. However, this means that 67.3 percent of the population remained offline (DataReportal, 2023).[58] With this lack of widespread connectivity, the majority of individuals will be unable to access digital services meaning they will be unable to access digital financial services and remittances.

58 https://datareportal.com/reports/digital-2023-kenya

5.2 Asia and Oceania

Cross-border Initiatives	Countries Affected	Objective	Description	Status	Enablers	Challenges
Modular Open Source Identity Platform (**MOSIP**) (MOSIP)[59]	Ongoing (Philippines, Morocco, Ethiopia, Guinea, Togo). MoU (Sri Lanka, Burkina Faso, Niger, Madagascar, Sierra Leone, Uganda)	Legal identification	MOSIP is a modular and open-source identity platform that helps user organisations such as governments implement a digital, foundational ID cost-effectively.	Live (2020) – Functionality for cross-border there due to platform. However, not currently used.	• Enable local custom build, zero-knowledge architecture to ensure no possibility of fraud or theft • Has interoperability that enables cross-border operation • Enable digital identity for the digital economy	• Lack of an ID system in some African countries • Internet connectivity issues • The system had to be customized to local needs due to different languages used in various countries • No interoperable use cases currently exist
Association of Southeast Asian Nations (**ASEAN**) – Digital Integration Framework (Asean, 2020)[60]	10 Member States (Brunei Darussalam, Cambodia, Indonesia, Lao PDR, Malaysia, Myanmar, Philippines, Singapore, Thailand, Vietnam)	Cross-border digital trade	To build on existing national digital ID systems to encourage the adoption of digital FS by enabling real-time and secure verification of user identities	MOU – Brunei, Indonesia, Malaysia, Singapore and Thailand are fully digitised, and others are in progress digitizing fID systems (2017)	• Enable digital payment to facilitate seamless cross-border digital trade and serve as a gateway to other digital financial services • Enable real-time and secure verification of user identities	• Digital divide • Lack of digital interoperability • Political differences and lack of collaboration efforts across leading ASEAN countries

59 https://mosip.io/
60 https://asean.org/wp-content/uploads/2020/12/Adopted-ASEAN-Digital-Integration-Framework.pdf

Cross-border Initiatives	Countries Affected	Objective	Description	Status	Enablers	Challenges
Memorandum of Understanding (**MOU**)	Singapore and Thailand (ASEAN Briefing, 2022)[61]	Cross-border digital payment/ trade	Singapore's PayNow and Thailand's PromptPay allow peer-to-peer transfers and cross-border payments using recipients' NID card numbers	Exploration (2017) Live (2021)	• The sender no longer needs to key in the name and bank account details of the recipient • The recipient will receive the funds within minutes • Affordable fees, transparently displayed to senders • Transactions screened in accordance with AML laws and regulations	• Ensure that this framework was legally binding and compliant with AML and CFT screening requirements in the context of two separate legal systems with different laws and regulations
	Singapore and Philippines (Philippine News Agency, 2023)[62]		Mutual recognition of the PhilID and Singapore's Singpass to allow each nation's digital ID to be recognized in the other's jurisdiction and promote interoperability among digital identity and related systems	Exploration (2022)	• Promote interoperability among digital identity and related system • Learn from Singapore's extensive experience with digital government services and cybersecurity	• In development • Need to cover knowledge and technical expertise on combatting fraud and protecting personal data under agreement
Frameworks on Cooperation (**FoC**) (Ministry of Trade and Industry Singapore, 2023)[63]	Singapore and Malaysia	Cross-border digital trade	Agreement to promote exchanges and knowledge-sharing to facilitate the interoperability and development of our respective digital identity regime Potential bilateral pilot on corporate Digital IDs as a proof-of-concept for The ASEAN Unique Business Identification Number Network (UBIN) system	FoC (2023)	• Expand areas of economic cooperation in the digital economy to keep trade flowing by facilitating interoperability between the two countries • Potential pilot of corporate digital identities	• Concept in development

61 https://www.aseanbriefing.com/news/thailand-and-singapore-sign-agreements-to-deepen-economic-cooperation/
62 https://www.pna.gov.ph/articles/1192927
63 https://www.mti.gov.sg/Newsroom/Press-Releases/2023/01/Factsheet-on-Frameworks-on-Cooperation-in-Digital-Economy-and-Green-Economy

Cross-border Initiatives	Countries Affected	Objective	Description	Status	Enablers	Challenges
Mutual Recognition of DI – Single Economic Market Agenda (Australian government)[64]	Australia, New Zealand	Cross-border digital trade	Agreements recognize digital identity services to have streamlined online interactions between individuals, firms and governments	In Development (2020)	• Support each country's long-term economic recovery and growth • Enable digital trade and other cross-border transactions (foster trust in online transactions) • Be the basis for mutual recognition of digital identity • Streamline online trans-Tasman interactions between individuals, firms and governments	• New Zealand is in the process of passing digital ID bills • Digital identity systems are not interoperable and reusable between organisations, government, and private sector

64 https://www.dfat.gov.au/trade/agreements/in-force/anzcerta/Pages/australia-new-zealand-closer-economic-relations-trade-agreement#:~:text=The%20agenda%20was%20endorsed%20at,can%20operate%20across%20the%20Tasman

Cross-border Initiatives	Countries Affected	Objective	Description	Status	Enablers	Challenges
Mutual Recognition of DI – Digital Economy Agreement	Singapore and Australia (Australian government, 2020)[65]	Economic cooperation, Cross-border digital trade	Australia and Singapore have entered into a dialogue regarding a mutual recognition agreement, potentially starting with students working on interoperability and policy frameworks	Exploration (2020)	• Explore principles of adopting open standards which support interoperability with different digital services and international partners	• Need to ensure that private and sensitive identity data is secure • Governments need to develop a holistic approach to using digital identity • Needs to focus on adequate cybersecurity protection for digital identity frameworks to ensure the protection of sensitive data and interlinked data from identity
	Singapore and UK (UK government, 2021)[66]		To develop a roadmap to enable the interoperability, mutual recognition and use of digital identities between the participants	Exploration (2021)	• Development of a joint roadmap which provides a plan of activities to reach mutual recognition of digital identities • Identification of scenarios and use cases and the design of pilots to support research into interoperability and mutual recognition of digital identities • Work toward mutual recognition of digital identity approaches, which would allow digital identities to be used for cross-border transactions	• Concept in development • The UK currently does not have a national ID system
Mutual Recognition of DI – EU-Singapore Digital Partnership (MTI, 2022)[67]	Singapore, EU	Cross-border digital trade	Singapore and the EU agreed on key priorities of implementation for 2023: exploring common approaches in e-identification to facilitate digital trade and SME's digital transformation	Trade Agreement (2022)	• Facilitate digital trade and SME's digital transformation • Strengthen countries' cooperation as strategic partners	• Concept in development – Exploring common approaches in e-identification • Yet to be defined what success looks like for partnership

65 https://www.dfat.gov.au/trade/services-and-digital-trade/australia-and-singapore-digital-economy-agreement
66 https://www.gov.uk/government/publications/memoranda-of-understanding-with-singapore-digital-trade-facilitation-digital-identity-and-cyber-security/memorandum-of-understanding-on-digital-identities-cooperation
67 https://www.mti.gov.sg/-/media/MTI/Microsites/DEAs/EUSDP/EU-SGP-Digital-Partnership.pdf

In the Asia region, countries have a medium level of maturity in national digital identity systems. There is mixed government appetite to expand or create national identity systems. Countries including Singapore, India and the Philippines stand out in their digital identity development, which is relatively mature and advanced.

Singpass, Singapore's national digital identity, allows users to transact with over 460 government agencies and private sector organisations across more than 1,700 services. It has a user base of more than 4.2 million users, which cover almost 100 percent of Singapore's population, including foreigners, when their work and residences are approved (Singapore Government Development Portal).[68] The private sector uses Singpass to enable paperless, digital and instant opening of bank accounts, credit cards, loans and insurance applications. To further drive private sector adoption, the Monetary Authority of Singapore guided that using Singpass meets certain document requirements for AML/CFT customer due diligence (CDD) (MAS, 2022).[69] On the other hand, Aadhaar in India is deemed to have strong adoption of over 1 billion users covering 95 percent of the population and has been established to address social exclusion and achieve broader economic goals (Canadian Bankers Association, 2018).[70] The implementation of Aadhaar provides legal identity to residents, including individuals who have resided in India for 182 days or more in 12 months, to obtain welfare benefits, reduce corruption, intermediation and agency costs, and avoid identity fraud (The Economic Times, 2018).[71] As of June 2021, 1.2 billion out of 1.4 billion bank accounts in the country were linked to Aadhaar, enabling eligible residents, including migrants fulfilling residency requirements, to enter the formal financial system (NewsOnAir, 2022).[72] Despite the successful adoption, there were concerns over security and privacy throughout the roll-out.

The Philippines is also progressing in the digital identity space with its foundational digital ID system – PhilSys – built on the Modular Open-Source Identification Platform (MOSIP), which has enrolled more than 72 million residents as of August 2022 (Philippine Statistics Authority).[73] Although the Philippines came across issues of connectivity in terms of implementation, PhilSys serves as a foundational ID system enabling the proof of identity as a means of simplifying public and private transactions, promoting social service delivery, strengthening financial inclusion, as well as accelerating the digital economy. With mobile registration reaching far-flung areas, the National Statistician and Civil Registrar General indicated that they are on track to achieve improved access to financial and social protection services, especially for low-income individuals. Since MOSIP has interoperability, it could potentially be leveraged for cross-border digital identity acceptance between countries or migration corridors that built their digital identity system on the same platform.

Putting the spotlight on the Oceanic region, both Australia and New Zealand do not have a national identity card policy but have started to develop their own digital identity programmes. In Australia, the new digital identity ecosystem is expected to make it easier for businesses to verify customer identities without collecting excessive personal information, and the federal government is expected to introduce legislation on the scheme by the end of 2023 (Biometric Update).[74] As part of the public and private partnership, Mastercard has also been piloting its digital identity verification service in Australia, expressing support for the proposed system. Mastercard gained accreditation from the Australian government as a provider of digital ID credentials and Level 1+ identity proofing services under the government's Trusted Digital

68 https://www.tech.gov.sg/files/media/media-releases/Media%20Factsheet%20on%20Singpass%20(National%20Digital%20Identity)_28%20October%202021.pdf
69 https://www.mas.gov.sg/-/media/mas-media-library/regulation/circulars/amld/circular---non-face-to-face-customer-due-diligence-measures-1.pdf
70 https://cba.ca/Assets/CBA/Documents/Files/Article%20Category/PDF/paper-2018-embracing-digital-id-in-canada-en.pdf
71 https://economictimes.indiatimes.com/wealth/personal-finance-news/who-are-eligible-to-apply-for-aadhaar-find-out/articleshow/59998036.cms?from=mdr
72 https://newsonair.com/2022/01/04/aadhaar-going-global-the-potential-point/
73 https://psa.gov.ph/content/72-million-filipinos-now-registered-philsys
74 https://www.biometricupdate.com/202302/australia-and-state-govts-agree-on-digital-id-credential-sharing-deal

Identity Framework (TDIF) (Biometric Update, 2023).[75] New Zealand, meanwhile, is also in the development of its digital identity programme based on the digital identity Services Trust Framework, aligning with Australia, Canada and the United Kingdom. The government aims to build resilience, support the country's long-term economic recovery and growth, and enable digital trade and cross-border transactions with digital identity capabilities (Government of New Zealand).[76] New Zealand is currently reviewing the Digital Identity Services Trust Framework Bill, which will be a legal framework providing secure and trusted digital identity services for individuals and organisations (New Zealand Parliament, 2023).[77]

In terms of cross-border initiatives, the Association of Southeast Asian Nations (ASEAN) digital integration framework was established in 2019 to set priorities for Member States to accelerate digital integration, which includes enabling seamless digital payment by developing or building on existing national digital ID systems to encourage adoption of digital financial services with real-time and secure verification of user identities (Asean, 2020).[78] Singapore has been one of the leading countries actively involved in cross-border collaborations by exploring use cases, such as opening individual and business bank accounts and applying for work permits, passports and driving licenses while aligning to international standards (Digital Government Exchange, 2022).[79] Its efforts have been observed in the agreements it has signed with Malaysia, the Philippines, Australia, the UK, the EU and Canada to advance the mutual acceptance of digital identity by the governments and private sector (UK government).[80]

From Asia and Oceania, the top three challenges for providing digital identity and enabling it across borders are as follows:

1. **A limited number of countries with existing national digital identity solutions in the region**. While Singapore and India have two world-leading digital identity solutions, many other countries in this region fail to have such a solution that meets the needs of their citizens. While Oceania is advancing with new trust frameworks and international agreements, Southeast Asian markets are at different stages of digital identity development. Although some progress has been made, these markets still need to address challenges such as data security and privacy, data consistency, and, particularly, corruption.

2. **Many countries in Asia lag in digital and internet infrastructure, inhibiting the use of digital identity**. According to the Asian Development Bank (ADB), it is estimated that Asia will need to invest around US$1.7 trillion each year in infrastructure until 2030 to sustain economic growth, combat poverty, and address climate-related challenges (ADB, 2017).[81] This required investment is more than double the amount recommended by the ADB back in 2009. Consequently, the disparity between the projected infrastructure requirements and the actual infrastructure development is expanding.

3. **Lack of digital privacy and data flow interoperability**. The limited regional collaboration in Southeast Asia (SEA) stems from the absence of interoperable systems and frameworks spanning border regions and different countries. When it comes to data privacy and security, SEA nations have adopted diverse approaches, with certain governments aiming to control the movement of data across borders. Notably, Vietnam and Indonesia have implemented the most extensive restrictions on data flows within ASEAN. Achieving consistency in

75 https://www.biometricupdate.com/202207/xydus-mastercard-gain-digital-id-trust-accreditations-in-uk-Australia
76 https://www.digital.govt.nz/digital-government/programmes-and-projects/digital-identity-programme/problems-benefits-and-outcomes/
77 https://bills.parliament.nz/v/6/b00cd25e-18dd-48d7-a68a-047aa9f41fce?Tab=history
78 https://asean.org/wp-content/uploads/2020/12/Adopted-ASEAN-Digital-Integration-Framework.pdf
79 https://www.developer.tech.gov.sg/our-digital-journey/digital-government-exchange/files/DGX%20DIWG%202022%20Report%20v1.5.pdf
80 https://www.gov.uk/government/publications/memoranda-of-understanding-with-singapore-digital-trade-facilitation-digital-identity-and-cyber-security/memorandum-of-understanding-on-digital-identities-cooperation
81 https://www.adb.org/publications/asia-infrastructure-needs

strategies, policies, and systems at the regional level can enhance cross-border public services and e-commerce (Brookings, 2020).[82]

Bangladesh Use Case

Bangladesh has successfully implemented a foundational national identity system, with over 80 percent of its population registered. This system revolves around the issuance of the National Identity Card (NID), a unique document exclusive to Bangladeshi citizens, serving as the primary means of identification. The NID plays a pivotal role in various aspects of life, including access to government services, conducting financial transactions, and participating in the electoral process.

In 2020, the Bangladesh Financial Intelligence Unit introduced guidance for Electronic Know Your Customer (e-KYC). This innovative approach allows banks and financial service providers (FSPs) to streamline the account-opening process. Customers can take pictures of the front and back of their NID card and submit a selfie. Subsequently, the bank or FSP verifies the NID and the customer's profile photo by automatically cross-referencing them with the National Election Commission database, facilitating the swift opening of customer accounts.

The main challenges behind digital identity and cross-border digital identity are as follows:

1 **Large technology infrastructure issues limit success**. Bangladesh's internet penetration rate stood at 31.5 percent of the total population at the start of 2022 (DataReportal, 2022).[83] Limited infrastructure and connectivity in some areas of the country pose challenges to the effective implementation of digital identity systems. Reliable internet connectivity and technological infrastructure are essential for seamless access to digital identity services, particularly in remote or rural areas where connectivity may be limited (Utilities One, 2023).[84] Efforts are needed to bridge the digital divide by addressing issues such as the affordability of devices, digital literacy, and language barriers to ensure that all citizens can benefit from digital identity services.

2 **Trust and security concerns with digital identity solutions**. In Bangladesh, recent surveys have suggested that trust in the Bangladesh government is declining, especially with many saying it declined heavily during the pandemic (North South University, 2016).[85] Recently, some digital identity initiatives for Rohingya refugees raised controversy, with allegations that these data were collected from the refugees and later shared with the Myanmar government without their informed consent. As with any digital system, ensuring data security and privacy is a critical concern. Safeguarding personal information stored in digital identity systems is essential to prevent unauthorized access, data breaches, and misuse of personal data. Strong security measures, encryption protocols, and adherence to privacy regulations are

82 https://www.brookings.edu/wp-content/uploads/2020/12/Development-Southeast-Asia-Ch2-Digital.pdf
83 https://datareportal.com/reports/digital-2022-bangladesh
84 https://utilitiesone.com/telecommunications-infrastructure-and-the-future-of-digital-identities
85 http://www.northsouth.edu/newassets/files/ppg- research/PPG_5th_Batch/1._MahadiCitizensTrustin_Public_Institutions_Exploring_Trust_in_Public_Officials_in_Bangladesh.pdf

necessary to protect individuals' rights and build trust in the digital identity ecosystem.

3 **No unified effort for one digital identity**: Digital identification has been on the agenda of the Bangladesh government's endeavours for Digital Bangladesh. However, in recent years, there have been various approaches by different government and private sector entities. In December 2019, Bangladesh initiated a digital identity programme with the global ID2020 Alliance. In April 2021, in partnership with ID2020 and the Gavi Vaccine Alliance, the government issued an RFP for a healthcare digital ID project. This initiative aims to provide biometric-linked digital IDs to infants during routine immunizations. In June 2021, the Bangladeshi government unveiled a project to provide unique digital IDs to students in Classes 6-12 through an integrated education information management system. Lastly, in September 2021, the Bangladesh Bureau of Statistics (BBS) announced plans to collect demographic and biometric data from all citizens, storing it in the National Population Register (NPR) and assigning each citizen a 16-digit digital identification number. (The Daily Star, 2021)[86] Without a unified effort for digital identity, none of these solutions will be able to gain mass adoption. Instead, the creation of several different projects may create different solutions for individuals to use, which creates further issues and keeps identities within silos that cannot be used outside of a sector or organization.

86 https://www.thedailystar.net/views/opinion/news/time-make-digital-identity-nationwide-reality-2919206

5.3 Europe

Cross-border Initiatives	Countries Affected	Objective	Description	Status	Enablers	Challenges
e-IDAS (Electronic identification and trust services) (European Commission, 2023)[87]	EU Member States	Digital services, Cross-border digital trade	The EU's e-IDAS regulation encourages each EU Member State to have a digital identification scheme in place. As of 2022, just 14 percent of key public services across all EU states allow cross-border authentication with e-ID due to various challenges.	Live (2016)	• e-IDAS is a key enabler for secure cross-border transactions • Help financial institutions meet their legal obligations in terms of know-your-customer, anti-money laundering and strong authentication of parties	• Lack of awareness • Limited amount and scope of notified e-ID schemes • Lack of relevant public services • Legal obstacles • Low number of cross-border use cases
e-IDAS 2.0 (European Commission, 2023)[88]	EU Member States	Cross-border digital trade, Security and privacy	EU Commission published on 3 June 2021 a legislative proposal that EU citizens will be able to prove their identity and share electronic documents from their "European digital identity Wallets", making it compulsory for EU countries to offer their citizens a digital ID and for public and private services to accept the new digital wallet.	In Development (2021)	• Strategy for shaping the EU's digital future envisages a universally accepted public e-ID • Ensure accessible, secure and trusted digital identity with access to a broad range of online services • Protect against cybercrime (e.g., identity theft, manipulation) • Advanced electronic signatures, electronic identification, cross-border interoperability, compliance with international standards	• Clarity on what success looks like • Assessment of continued relevance of 2014 Regulation • Consider user needs and technological and market developments
Diia Wallet (MFA Ukraine)[89]	Ukraine	Digital services, Identify verification	Diia wallet is used for storing credentials such as ID cards, payroll, business registration and residence records.	Live (2020)	• Allow the government to stay in touch with Ukrainians and rapidly introduce new forms of support • Diia holds payroll, business registration and residence records. Users can verify eligibility and apply for support directly in the app	• Cyber security problems in Ukraine • The level of technical literacy of the population • Data leak and privacy concern
Germany and Spain – **Mutual Agreement** (DigWatch, 2021)[90]	Germany, Spain	Cross-border digital services	The agreement was signed to develop a joint cross-border pilot programme for digital ID, enabling citizens to prove their identity and access public and private digital services in both countries	Exploration (2021)	• Adhere to data privacy as it will adopt a privacy-by-design approach • Institutions gradually become part of the national digital identity ecosystem based on the principles of self-sovereign identity (SSI) • Governments recognise digital identity as a fundamental building block for successful digitisation	• In development • Upscale identity ecosystem for cross-border use cases • Ensure safe and reliable digital ID based on state-issued ID documents

87 https://digital-strategy.ec.europa.eu/en/policies/eidas-regulation
88 https://digital-strategy.ec.europa.eu/en/policies/eidas-regulation
89 https://ukraine.ua/invest-trade/digitalization/
90 https://dig.watch/updates/spain-and-germany-will-test-cross-border-digital-identity

Delving into the digital identity landscape regionally, Europe is observed to be more mature compared to other regions. The European Commission has announced the initiative of the "European Digital Identity Wallet" to accelerate cross-border digital identity development to enable cross-border use cases, which is leading the industry and is the most advanced development in portable digital identity that can be accepted in multiple nation-states.

Countries such as Belgium, Estonia, France, Germany, and the Nordics have adopted digital identity with notified electronic digital identity schemes. In France, about 40 million citizens have adopted FranceConnect+ to authenticate and access over 1,500 online services, including accessing medical information and opening a bank account (In Cyber News, 2022).[91] Belgium's itsme® is another example of digital identity which allows citizens to access both social services via the government and financial services (itsme).[92] In the Nordics, bank-led digital identity systems allow citizens to leverage BankID to access public and private services. Successful domestic implementation of e-ID schemes can potentially be expanded to neighbouring countries, facilitating access to online services in other Member States through cross-border interoperability of national e-ID.

Estonia: digital identity adoption success story

Estonia, for example, excels in their digital identity rollout. It has an advanced digital identity framework upheld by the Identify Documents Act and Digital Signatures Act, ensuring Estonians are issued smart ID cards and laying the foundation for accepting digital signatures. Estonia built a data exchange layer called X-Road that allows the public and private sectors to securely exchange data and to ensure the information is compatible and up to date, enabling people to access a variety of services using their digital ID. Its success has been evidenced by X-Road's capability to save 800 years of worktime annually, connect over 900 organizations and database with more than 500 million transactions per year.

Despite several successful national implementations of digital identity observed, the adoption of key public services across all EU Member States allowing cross-border authentication with e-ID is still low at 14 percent (European Commission, 2021).[93] This is due to the lack of awareness of e-IDAS by citizens and e-IDs schemes by the private sector. In view of this, the European Commission published a legislation proposal in 2021 to make it compulsory for EU countries to offer their citizens digital identity and for public and private services to accept the new "European digital identity Wallet" to enable more cross-border use cases (Ex-Post Evaluation Unit, 2022).[94] The proposed legislation aims to reach a target of 80 percent of EU citizens using a digital e-ID solution by 2030, with measures including advanced electronic signatures, trust services, cross-border interoperability and compliance with international standards. One of the interviewees expressed positivity but also concern about the EU digital wallet, stating that "*e-IDAS 2.0 is pushing into private sectors to have more cross-border use cases, but without having more of a public and private partnership, there will be the same challenges there*."

Ukraine and Poland show a successful example of a national digital ID system accepted across the border. The Diia Wallet in Ukraine is an innovative national digital identity allowing citizens to access numerous services digitally. Due to the Russo-Ukrainian War, more than 7.8 million

91 https://incyber.org/en/digital-identity-toward-age-of-reason/
92 https://www.itsme-id.com/en-BE/why-itsme/security
93 https://commission.europa.eu/strategy-and-policy/priorities-2019-2024/europe-fit-digital-age/european-digital-identity_en
94 https://www.europarl.europa.eu/RegData/etudes/BRIE/2022/699491/EPRS_BRI(2022)699491_EN.pdf

people have fled Ukraine (Knomad, 2022).[95] The Diia Wallet allows the government to stay in touch with Ukrainians and provide support directly in the app. Diia is a centralized digital platform for storing, managing, and sharing official credentials such as vaccination records, insurance documents, passports, ID cards, and licenses. Despite the fact that there had been concerns about cybersecurity problems, technical literacy and data privacy about using Diia Wallet, the circumstances they are in have fastened the digital identity journey of Ukrainians. Ukrainian digital documents are gaining more and more recognition in Europe. For instance, Diia.pl, an electronic document issued to Ukrainian citizens who crossed the Polish-Ukrainian border, and a digital driver's license and technical passport that can be displayed in the Polish application mObywatel. The portability of digital identity, in this case, certainly brings benefits to those migrants and refugees moving from Ukraine in enhancing their ability to identify themselves to other organisations and access formal financial services.

It is encouraging to see developments in Europe, yet continued significant and sustained investment is still required. The revised e-IDAS regulation presents the opportunity for cross-border digital identity to become a reality, but it requires both the public and private sectors to work together to drive economic value for the region. Only when this is implemented and successful that the idea of using digital identity for cross-border remittances become a reality for those migrants that move within Europe.

From Europe, the top three challenges for providing digital identity and enabling it across borders are as follows:

1. **Limitations of e-IDAS 1.0.** The EU established e-IDAS regulation in 2014, encouraging Member States to acknowledge digital identity schemes from other EU countries. This is seen as a key enabler for secure cross-border transactions, helping financial institutions meet their legal obligations in terms of KYC, AML and strong authentication of parties. As of 2020, only 14 EU Member States had notified e-ID schemes that abided by regulation. That was about 60 percent of EU citizens who may benefit from cross-border electronic identification services, which is considered a relatively low level of application, especially since there were very few use cases for it to be used. Since there is no obligation for Member States to notify e-ID schemes under the 2014 e-IDAS Regulation, several Member States have chosen not to seek mutual recognition of their national e-ID schemes. Despite several successful implementations of digital identity observed, the adoption of key public services across all EU Member States allowing cross-border authentication with e-ID is still low at 14 percent (European Commission, 2021).[96] This is due to the lack of awareness of e-IDAS by citizens and e-IDs schemes by the private sector.

2. **Lack of private sector involvement and collaboration.** Even with the changes to the e-IDAS 2.0, the private sector and especially the financial services industry have questions over its use. In recent news, financial institutions and digital commerce entities in Europe are calling for clarification on some wordings used in the EU's digital identity Regulation (e-IDAS), which seems to make the application of the regulation mandatory for the full lifecycle of payments (Biometric Update, 2023).[97] Additionally, some respondents from financial service organizations were not completely sure of the process once the EU Digital Wallet becomes more mainstream, with some believing that they would still need to conduct their own identity verification, dependant on the scenario of the individual. Without this close collaboration throughout the EU, digital identity acceptance across borders in the financial services with falter and prove ineffective in its ambitions.

95 https://www.knomad.org/sites/default/files/2022-11/migration_and_development_brief_37_nov_2022.pdf
96 https://commission.europa.eu/strategy-and-policy/priorities-2019-2024/europe-fit-digital-age/european-digital-identity_en
97 https://www.biometricupdate.com/202306/eu-financial-associations-want-traditional-payments-excluded-from-eidas-regulation

3. **Digital identity usage is still relatively low.** Only five European nations have well-established digital identity initiatives, which are characterized by the active participation of over 40 percent of their citizens. While numerous European countries have introduced their own national digital identity programmes, the usage rates continue to be relatively low. Notably, the United Kingdom faces ongoing challenges related to trust and privacy in the realm of digital identities. Meanwhile, certain southern European states, such as Greece, Bulgaria, and Romania, are yet to enact such policies (Tech Monitor, 2022).[98] While the revised e-IDAS framework will assist in creating the correct infrastructure to allow digital credentials to work across borders, it will be ineffective if states and governments do not provide the ability for individuals to be given such identity credentials in order to access greater efficiencies.

Germany use case

Since the 1900s, the German government has been issuing identity cards to its residents. However, starting in 2010, these identity cards transitioned into electronic ID cards or e-IDs. The initial expectation was that e-IDs would become the primary means of identification for German citizens, both in the public and private sectors. However, progress toward this goal has been slow, with only 6 percent of the German population actively utilizing the card's electronic features (CEIC, 2021).[99]

One significant factor contributing to this limited adoption is the strong emphasis on privacy awareness among the German population. Many individuals in Germany are cautious and hesitant about sharing personal information online. Some fear that e-IDs grant the government too much access to citizens' data, citing concerns related to data protection regulations as a key reason for their reluctance to embrace these electronic IDs.

Furthermore, the private sector has been slow to adopt e-ID solutions for several reasons. Integration of digital identity solutions within organizations has proven to be challenging, and there is a lingering question about the value these solutions would bring to internal operations.

The main challenges behind digital identity and cross-border digital identity are as follows:

1 **Issues with current German digital ID solutions and their compatibility.** The current German Digital ID solution does not have the capabilities required by e-IDAS 2.0 and will require improvements. At present, it would not be easy to take German e-ID data and move it to another EU DI wallet, for example, in Sweden. This is a large challenge before the country can reap the benefits of a cross-border digital identity.

2 **Lack of awareness and education.** Extensive research has highlighted the existing potential for significant advancements in the utilization of digital services within Germany. Despite the growing prevalence of digitalization, a notable proportion of users in the country continue to favour traditional analogue procedures over their digital counterparts. This

98 https://techmonitor.ai/focus/the-state-of-digital-identity-in-europe
99 https://www.ceicdata.com/en/germany/telecommunication/de-internet-users-individuals--of-population#:~:text=Germany%20DE%3A%20Internet%20Users%3A%20Individuals%3A%20%25%20of%20Population%20data,to%202021%2C%20with%2032%20observations

preference for analogue methods can be attributed to several factors, including apprehensions related to security and safety in the digital realm. Many individuals remain cautious about entrusting their personal information and transactions to digital platforms, fearing data breaches and cyber-threats (IDNow, 2023).[100]

3 **Slower to Digitalization than other EU Countries.** Only 50 percent of Germans possess basic digital skills – compared to 80 percent of Finns (CEPA, 2022).[101] Additionally, the European Union's Digital Economy and Society Index, which monitors digitization efforts across the bloc, ranks Germany only 13th among the EU's 27 member countries (European Commission, 2023).[102] With Germans slow to adjust to digital transformation, there is no guarantee that the EU Digital Wallet will create further adoption in their digital identity efforts.

100 https://www.idnow.io/blog/digital-identity-index-2023-study-future-germany/#:~:text=Our%20Digital%20Identity%20Index%202023,the%20existence%20of%20digital%20services

101 https://cepa.org/article/deutsche-katastrophe-germany-fights-digital-backwardness/

102 https://digital-strategy.ec.europa.eu/en

5.4 North and South America

Cross-border Initiatives	Countries Affected	Objective	Description	Status	Enablers	Challenges
Colombia **Digital Passport** (NFCW, 2022)[103]	Colombia, Argentina, Bolivia, Brazil, Chile, Ecuador, Paraguay, Peru and Uruguay	Free movement of people, Security	Colombia originally launched the Cédula Digital in 2020. The upgrade to the Cédula Digital "complies with high international standards" and will enable Colombians to create a digital version of their national ID card on their smartphone to verify their identity using facial recognition when travelling to Argentina, Bolivia, Brazil, Chile, Ecuador, Paraguay, Peru and Uruguay	Live (2022)	• Create a digital version of a national ID card on a smartphone by downloading an app from the National Registry of Civil Status • Authenticate identity using facial recognition on a smartphone • Cédula Digital can be used as a digital passport for cross-border travel	• Half of the population lacks access to internet • Security concerns about current Colombian ID card
MERCOSUR Countries – **Mutual recognition of national IDs** (World Bank)[104]	Argentina, Brazil, Paraguay and Uruguay	Free movement of people, Cross-border trade	MERCOSUR countries have expanded freedom of movement for all its citizens, allowing them to travel with the use of an ID card, enabling key use cases of migration	Live (2017)	• Facilitate the integration and mobility of citizens, goods and services within the MERCOSUR region • Ensure the security and protection of personal data	• Limited on accessing public services and contactless cross-border travel • Currently not digital – requires physical identity cards • Apart from travel, no further use cases have been identified
Uruguay's **e-ID cards** (Thales)[105]	Uruguay	Free movement of people, Digital services	Uruguay's e-ID cards are the official travel documents for Uruguayan citizens within the Mercosur and associated countries by being ICAO-compliant, enabling the use of digital signatures among other government initiatives	Live (2015)	• Prove citizens' identity online for government and private services • Stronger online authentication and includes capabilities to simplify e-government initiatives • Benefit from exceptional security when using ID documents or travelling abroad	• Build a reliable Public key infrastructure for the digital signing of sensitive biometric data for cardholders in compliance with ICAO recommendations • Achieving the highest level of protection for e-ID card and e-passport holders

103 https://www.nfcw.com/2022/08/10/378486/colombia-to-let-citizens-use-digital-id-for-contactless-cross-border-travel-in-south-america/
104 https://id4d.worldbank.org/guide/mutual-recognition-ids-across-borders-0#:~:text=In%20Latin%20America%2C%20for%20example,and%20Uganda%20in%20East%20Africa
105 https://www.thalesgroup.com/en/markets/digital-identity-and-security/government/customer-cases/uruguay-eid

Cross-border Initiatives	Countries Affected	Objective	Description	Status	Enablers	Challenges
Brazil's **e-ID cards** (KPMG, 2022)[106]	Brazil	Free movement of people, Digital services	Residents can now generate a digital national identity card stored on their smartphone and use it to verify their ID for multiple uses, including accessing public services and contactless cross-border travel to other South American countries within the Mercosur region	Live (2015)	• Store the digital ID on an Apple or Android smartphone • Easy access to public services and contactless cross-border travel to other South American countries within the Mercosur region • Enable a single standard throughout the country	• Concern about digital service security due to experiences of being hacked, reducing overall trust in networks and e-commerce sites for managing citizens' personal data • Concern about the National Identity System and the country's data protection rules and principles • Possibility of generating exclusion if poorly implemented • Concern about government surveillance
Cross-border acceptance of digital ID (Government of Canada, 2021)[107]	Canada and EU	Exploration of cross-border digital credentials	A partnership between the government of Canada and the European Commission to examine the use of digital credentials: (i) the current technology and policy landscapes, (ii) areas of commonality and gaps that need to be addressed to enable mutual support for the use of digital credentials	Exploration (2021)	• Potential to establish a trust framework that could enable interoperability • Increase security, efficiency, privacy and accessibility for individuals, businesses and organizations operating online	• Different standards across different economic sectors and jurisdictions • Disparate systems leading to challenges for mutual recognition and scalability of digital credential systems • Lack of standards for digital wallets

106 https://kpmg.com/xx/en/home/insights/2022/07/flash-alert-2022-135.html
107 https://www.canada.ca/en/innovation-science-economic-development/news/2021/11/government-of-canada-announces-partnership-with-the-european-commission-to-examine-the-use-of-digital-credentials.html

Cross-border Initiatives	Countries Affected	Objective	Description	Status	Enablers	Challenges
Cross-border acceptance of digital ID (Digital Policy Alert, 2021)[108]	Canada and UK	Exploration of cross-border digital credentials	Partnership between Canada and the UK to explore digital credentials established.	Exploration (2022)	• Potential to establish a trust framework that could enable interoperability • Establish a common understanding of the digital credentials model • Enable cross-border interoperability and mutual support for digital credentials and digital trust services	• Regulatory and technology gaps • Exploring use cases for proof of concepts or pilot
State IDs or Driver's License digital wallets (Thales)[109]	US	Financial identification, Digital Economy	Apple rolled out the ability for US residents to seamlessly and securely add their driver's license or state ID to Wallet on their iPhone and Apple Watch, enabling a more seamless airport security screening experience for travellers	Live (2021)	• Secure storage of sensitive information • Safer identification and payment processes • Improved control over data sharing • Simplified transactions and convenient for users • A unified and transparent system available across different jurisdictions • The absence of the need to carry printed documents	• Competition of interests between governments and tech giants • Privacy Concerns

108 https://digitalpolicyalert.org/change/1330-digital-identity-requirements-in-uk-canada-agile-nations-digital-credentials-project
109 https://www.thalesgroup.com/en/markets/digital-identity-and-security/government/mobile-driver-licence

Within North America, the level of maturity in digital identity systems is medium with moderate government appetite to create digital identity programmes. In the US and Canada, the level of adoption of digital identity varies across states or provinces due to its implementation being largely at the state or provincial level. While in Mexico, the government has accelerated its ID issuance since 2014, generally for account opening and U.S. businesses due to the importance of the United States-Mexico-Canada Agreement (USMCA) corridor (Trulioo, 2020).[110] There is no standardised approach toward digital identity across this region. However, Canada is progressing to establish trust frameworks at a national level and engaging in cross-border initiatives with other countries such as the EU and the UK.

In Canada, there is not yet a national ID system, but a Pan-Canadian Trust Framework (PCTF) developed through public-private collaboration and published by the Digital Identification and Authentication Council of Canada (DIACC). These are based on a robust approach to the privacy, safety and security of citizens, federated identity models, open technical standards, and a mix of self-certification and independent certification processes (OIX, 2020).[111] To extend its collaboration with the private sector, the DIACC has also launched a trust certification programme called Voila Verified, which is a third-party conformity assessment programme that verifies compliance of solutions and services against the criteria defined in the PCTF (DIAAC, 2022).[112] One of the main challenges encountered by Canada's digital identity programme is its governance model, in which the provinces and territories issue the majority of authoritative foundational records. Given the model of distributed governance, there is no single authoritative policy-making body in Canada.

In terms of cross-border collaborations, Canada has been actively involved in digital identity in the Digital Government Exchange (DGX) digital identity Working Group (DIWG) in response to COVID-19 and the Know Traveller digital identity (KTDI) to enhance security in world travel (Digital government Exchange, 2022).[113] DIACC indicated that the PCTF may be extended and applied outside of Canada. Partnerships have been established with the EU, the UK, and the Netherlands to explore cross-border acceptance of digital identity. With the European Commission, Canada aims to examine the use of digital credentials with a series of workshops examining current technology and policy landscapes, identifying areas of commonality, and enabling interoperability and mutual support for digital credentials (Government of Canada, 2021).[114] Canada is also leading Digital Credentials and Digital Trust Services, supported by the UK and observed by Italy and Singapore to establish a common understanding of the digital credentials model and how it could be applied to use cases of interest to Agile Nations members and to identify gaps in interoperability (UK government, 2022).[115]

110 https://www.trulioo.com/blog/identity-verification/business-mexico
111 https://canada-ca.github.io/PCTF-CCP/docs/RelatedPolicies/Blueprint-for-National-International-Oversight-of-the-Digital-Identity-Market-March-2020.pdf
112 https://diacc.ca/voila-verified/#:~:text=A%20Voil%C3%A0%20Verified%20Trustmark%20signals,meet%20international%20standards%20and%20regulations
113 https://www.tech.gov.sg/files/media/corporate-publications/FY2021/dgx_2021_digital_identity_in_response_to_covid-19.pdf
114 https://www.canada.ca/en/innovation-science-economic-development/news/2021/11/government-of-canada-announces-partnership-with-the-european-commission-to-examine-the-use-of-digital-credentials.html
115 https://www.gov.uk/government/publications/agile-nations-progress-report-2020-to-2022/agile-nations-2020-2022-progress-report#digital-credentials-and-digital-trust-services

Agile Nations

The Agile Nations is an inter-governmental regulatory cooperation network of 7 countries that focuses on practical collaboration on emerging technology. The countries involved are Canada, Denmark, Italy, Singapore, Japan, UAE, and the UK (UK government).[116]

In the US, the evolution of digital identities has been showcased in the innovation of digital wallets storing the digital version of State IDs or Driver's License (DL). Apple rolled out the ability for US residents to add their DL or state ID seamlessly and securely to Wallet on their iPhone and Apple Watch, enabling a seamless airport security screening experience for domestic travellers. This initiative provides an additional level of convenience for travellers by enabling touchless Transportation Security Administration (TSA) airport security screening (Apple, 2021).[117] Digital credentials are enabled through the route of having physical identity cards or a digital version on mobile devices. The TSA-approved digital ID is positioned for seamless travel but not for facilitating client onboarding and access to financial services.

Regarding the development in South America, Mercosur countries such as Argentina, Brazil, Colombia, and Uruguay have implemented digital identity programmes for easy and secure access to public services, as well as facilitating the mobility of citizens across the region. This has been particularly expedited by the Mercosur Agreement on mutual recognition of identities, which allows the use of digital identities within the region for cross-border travel (World Bank).[118] Currently, the process requires physical identity cards in some countries. Nonetheless, the recognition of identity cards from fID systems benefits the integration of regional blocs as they are more accessible than a passport. Uruguay's e-ID cards not only serve as the official travel documents within the Mercosur and associated countries by being ICAO-compliant but also enable the use of digital signatures among other e-government initiatives. Brazil has taken a step further, where residents can generate a digital national identity card to store on their smartphone and verify their ID for multiple uses, including accessing public services and contactless cross-border travel countries within the Mercosur region (NFCW, 2022).[119] Similarly, cross-border digital identity initiatives in the region focus on the free movement of people with limited exploration of cross-border use cases with private sectors such as opening a bank account or remittances.

From North and South America, the top three challenges for providing digital identity and enabling it across borders are as follows:

1. **Lack of public trust in digital identity and safeguarding of personal data.** One key thing that came from respondents and was particularly pertinent in this continent was related to trust. While there are some successful digital identity solutions within South America, within the whole region there has been limited success. Respondents believed that a key reason for this was a lack of public trust in digital identity. In one country within the region, they surveyed citizens, and it showed that 55 percent feel that digital identity has a positive impact on their lives, and 23 percent remain unsure about the impact of digital identity on their lives. Digital identity has also been referenced quite heavily in recent misinformation and disinformation that is spreading through unauthenticated networks such as Twitter, Facebook, and Reddit. Without this trust, citizens will rely on the existing solutions to prove their identity despite them potentially being less secure and more cumbersome.

116 https://www.gov.uk/government/groups/agile-nations
117 https://www.apple.com/newsroom/2021/09/apple-announces-first-states-to-adopt-drivers-licenses-and-state-ids-in-wallet/#:~:text=%E2%80%9CThe%20addition%20of%20driver%27s%20licenses,Apple%20Pay%20and%20Apple%20Wallet
118 https://id4d.worldbank.org/guide/mutual-recognition-ids-across-borders-0
119 https://www.nfcw.com/2022/11/10/380218/brazil-begins-rollout-of-contactless-mobile-identity-cards/#:~:text=Residents%20of%20six%20Brazilian%20states,travel%20to%20other%20South%20American

2. **Different governance models from country to country create Issues.** Successful digital identity solutions require a robust governance model to ensure that every stakeholder within the ecosystem understands their role and how identity credentials are issued, accepted, and stored, in addition to data management principles. However, while manageable for individual countries, when it comes to using digital identity across borders it becomes difficult as it requires such governance structures to become interoperable and co-exist. However, in large countries with multiple jurisdictions, such as Canada and the USA, these challenges exist within single countries. For personal identity, most authoritative foundational records are issued by the provinces, territories and states. Given this model of distributed governance, there is no single authoritative policy-making body, which makes it difficult to create and establish such an infrastructure for digital identity to become universal in these countries. Stronger links are required between all stakeholders within these countries, with common oversight to create such a framework that all such areas adhere to.

3. **Security, fraud and privacy challenges.** One such challenge that became apparent when looking deeper, especially at South America, was that of the security of data. Recently, the Brazilian Ministry of Health was the target of a security breach that exposed the data of more than 243 million Brazilians on the internet, while in 2020, Brazil accounted for 45.4 percent of global cases of credit card fraud (Forbes, 2021).[120] Such issues make it increasingly difficult for other governments and organizations to be able to work with countries that experience these data challenges because of the increased risk.

Colombia use case

Colombia has had national identity cards in place since the 1950s, but a significant digital transformation occurred at the close of 2020 with the implementation of a digital identity equivalent. The primary objective was to introduce a new electronic and digital ID system that could offer a high level of security and reliability in accessing digital public services. This initiative was part of a broader government digital transformation programme, marked by its swift and efficient implementation, promising positive opportunities. The newly introduced digital identity can be securely stored on individuals' mobile phones, facilitating both online authentication through biometrics and in-person verification via dedicated verification facilities.

Initially designed for public sector use, the government has been actively working to involve private sector organizations. In 2023, the government initiated various pilot programmes in collaboration with several banks. These pilots explored the use of facial authentication, allowing customers to conduct remote transactions from their home computers or mobile devices. The facial biometrics were compared to the national digital ID for enhanced security.

In addition to the government's efforts, three major banks in Colombia have joined forces to create "Soy Yo." This innovative platform enables individuals who already have bank accounts to access services at other organizations without the need for repeated identity verification. This collaborative approach streamlines processes and enhances convenience for users across various sectors.

120 https://www.forbes.com/sites/forbestechcouncil/2021/06/02/understanding-the-significance-of-digital-identification-problems-in-latin-america/?sh=1c025e74525f

The main challenges behind digital identity and cross-border digital identity are as follows:

1 **Lack of adoption.** What is evident is that mass adoption is the biggest challenge. Currently, there are not large amounts of services available with digital identity, but this is changing with work going into expanding its use into the financial services sector. As more services are available through digital identity, more people would be incentivized to use it and adopt it. The government need to get more involvement from the private sector by showcasing the potential to optimize processes and reduce costs through digital identity.

2 **Minimal private-public collaboration decreases valuable use cases.** Private-public collaboration in digital identity brings together the strengths of both sectors to create robust, secure, user-friendly, and scalable solutions. It harnesses the innovation and resources of the private sector while ensuring that the interests of governments and citizens are protected through regulation and oversight. In Colombia, there is still a disconnect behind this collaboration. Respondents from the financial services industry hoped for greater discussions in the future, with many of the banks looking to create their own solutions (see Soy Yo above). This may present problems in the future with them both competing for adoption from citizens unless they can work together and integrate both solutions for the benefit of the public.

3 **The technical infrastructure is still lagging.** In many countries that are developing at various stages, digital infrastructure and connectivity are suboptimal. Despite investments since 2000, there is still a gap between rural and urban areas within the country. While internet access reaches around 70 percent of the population, for many, going online is still too expensive and often slow. However, the government has recognized this, and in 2023, the ICT ministry announced a strategy to connect 85 percent of the country in four years. The plan will impact 1,122 municipalities in 32 departments.

6. RECOMMENDATIONS

Through the analysis of the global landscape, the various challenges to enabling digital identity across borders have been documented. Following this and including some ideas and thoughts from KII insights, recommendations have been formulated per type of stakeholder and geography.

6.1 Global Recommendations

All Stakeholders

- **Create opportunities for 'safe' sandbox environments/potential pilots/proof of concepts which equally benefit all parties involved.** Sandboxes provide a controlled environment where innovators, both from the public and private sectors, can experiment with new technologies and approaches related to cross-border digital identity. This promotes innovation and the development of more efficient and secure identity solutions while allowing the chance for all stakeholders to learn and understand what is required.
- **Contribute to agreeing to a trust framework or ISO standard for digital identity within a financial services context that meets consumer needs.** An optimal digital identity ecosystem requires many actors and roles. A trust framework is a rulebook that all ecosystem users should adhere to. It defines who is part of the ecosystem and how they can formally join, and identifies the identity issuers, verifiers and other parties. Rules should state which standards bodies are involved from each industry and how they should create uniform approaches for participants. These frameworks should detail how an auditor would assess the adequacy of system controls and recommend changes, as well as how the relevant regulators implement and enforce compliance at domestic, regional or international levels.
- **Increase engagement in international standardisation efforts.** While creating a set of regulations and standards that allow digital identity to work globally is the end goal, this presents a huge challenge that will take years to become a reality. Ideally, standards and harmonization should be done at the global level, as evidenced by ICAO (passport format harmonization) and the Digital Travel Credential initiative that will shape how virtual passports will be accepted across borders. But existing regional blocs and large migration corridors can already start to work through interoperability issues and create a trust framework to allow for its use will be an easier route to make cross-border acceptance a reality. These regional blocs can then work together to develop further relationships and mutual agreements to grow this. Eventually, a range of stakeholders, such as governments, financial service organizations, also NGOs and IGOs such as the FATF, should contribute to creating global standards behind digital identity with a common taxonomy in language. This should be done on specific use cases that prove worthwhile, such as financial service onboarding for migrants. A potential future solution could be to digitalize passports, utilizing the system currently in place and adding more use cases on top of the cross-border use.
- **Invest in and drive coordinated/unified cross-sector campaigns on improving digital literacy and access to education and increase digital inclusion.** Investing in and driving coordinated cross-sector campaigns to improve digital literacy, access to education, and increase digital inclusion is crucial for addressing the digital divide and ensuring equal opportunities for all. Without closing this gap, many individuals will be unable to access the value of utilizing digital identity and digital services. Governments should look to implement policies that support digital inclusion and equitable access to education while also working with financial service organizations to understand what is required to help those will less access to digital access such services. NGOs, with their global outreach, can translate and adapt digital literacy content into local languages to make it more accessible and relevant to the target audience while also directly facilitating the distribution of computers, tablets, and other devices to underserved communities.

Governments and Regulators

- **Lead efforts to convene diverse stakeholder audiences to discuss potentially viable models and create international agreements.** Governments must work not only within their geographical boundaries but work with other governments within their regions to create potential governance models behind cross-border digital identity acceptance. Governments can look to take inspiration from the EU's e-IDAS 2.0 regulation as to what is required.
- **Create 'safe' sandbox environments for testing and assurance.** Governments and regulators could further take action to create 'safe' sandbox environments for public and private sector testing and assurance purposes, and to promote the design of cross-border digital identity solutions that consider data privacy and security.
- **Invest in creating incentives for mutually beneficial collaboration/common infrastructure that reduces data silos.** Mutual collaboration can lead to the development of standardized security protocols and best practices. A common infrastructure can incorporate robust encryption methods and authentication mechanisms, making digital identity systems more secure.
- **Protect citizens via policy/frameworks, e.g., data minimisation principles, privacy, and anti-surveillance.** Develop identity frameworks that prioritize the interests of individuals. Citizens should have the ability to manage and control their digital identities, including the ability to revoke consent and delete their data. Governments should also mandate transparency in how digital identity systems operate, and organizations should be accountable for their actions and provide individuals with clear information about how their data is used. Especially when looking at biometric enrolment of individuals, governments will need to ensure safeguarding through such methods as data encryption, secure storage, and tokenisation among others. Additionally, a decentralized digital ID setup can help ensure the privacy of data by equipping citizens with devices to store data with themselves and disclose only when requested by trustable parties.
- **Provide consumer advice alongside a wider inclusion agenda to help migrants understand digital FS and Digital ID interlocks.** Develop and distribute consumer advice materials in multiple languages commonly spoken by migrants. This ensures that information is accessible and understandable to a diverse audience. In addition, they should establish community outreach programmes that engage with migrant communities directly. These programmes can include workshops, seminars, and information sessions to educate migrants about digital financial services and digital IDs. In addition to this, governments and regulators should work with financial service organizations to understand the issues with onboarding migrants from a company perspective and prioritize changing policies to support a more efficient and easier approach.
- **Support innovative approaches to enable ID issuance.** Allocate government funding or grants to support research and development in the digital ID space. Financial support can help startups and innovators bring their ideas to fruition, especially in particular geographies such as Africa, where mobile network operators are providing identities to individuals thanks to the outreach of mobile phones, as opposed to access to the internet and physical identities. Governments should ensure that these new approaches have the right level of assurance to ensure that organizations can trust the attestations made and they can be comfortable accepting them. In addition, identities should be designed with inclusivity in mind to ensure that everyone, including marginalized populations, has equal access to digital identity services, even when they have little to no access to offline resources.
- **Enforce regulation on informal channels for sending remittances and educate citizens on risks associated with informal providers and benefits of formal channels (e.g., accessing other products).** Governments should look to review and update existing laws and regulations to make them more robust and capable of addressing emerging challenges posed by informal channels. In addition, they should launch comprehensive public awareness campaigns to educate citizens about the risks associated with informal providers and integrate financial literacy into the wider society through community outreach and

school curriculum.

- **Strengthen political/commercial bilateral ties across major migration corridors.** Foster political dialogue and diplomatic engagement between countries along major migration corridors. Through regular high-level meetings and discussions, governments can help build trust and understanding and work toward cooperation and potential digital identity agreements between countries to create mutual economic benefits.

Financial Service Providers

- **Actively contribute to the discussion on the advantages and disadvantages of diverse solutions and educate/advise on the latest technology.** Financial Service Providers must work together to help governments get an understanding of the requirements for digital ID solutions and the role they must play within the ecosystem. This will assist in allowing all stakeholders to understand the current challenges financial services organizations face during the onboarding process within the current regulations such as KYC and AML. Working together, they can implement new measures and provide their understanding of new technologies that benefit all parties, especially their customers.
- **Revise risk management frameworks to align with the digital landscape.** Financial Service Providers should consider how changing risks could be accounted for within their risk management frameworks. Learnings from sandbox environments should be promptly transferred to revise risk management frameworks to align to new digital landscapes that address data protection, consent, and the responsible use of customer data to build trust with customers and enable digital identity as a "public good".
- **Identify and invest in mutually beneficial collaboration opportunities with institutions of different scales.** Cross-sector collaboration can lead to holistic digital identity solutions that cater to diverse user needs. Such collaborations can harness diverse expertise, pool resources, reach a broader user base, and foster adaptability, resulting in more effective and inclusive digital identity solutions. These collaborations should be supported by a combination of government initiatives, industry partnerships, and innovation ecosystems to ensure their success and widespread adoption.
- **Invest in customer journey transformation and ensure its success for migrants.** Embrace digital transformation by adopting the latest technologies, such as artificial intelligence, machine learning, and automation, to streamline operations, enhance data analytics, and personalize customer experiences. This will help invest in improving the entire customer journey, from onboarding to ongoing interactions and support. Additionally, organizations should ensure that digital identity platforms and information are available in multiple languages to accommodate migrants from diverse backgrounds while helping migrants to have access to the necessary technology, such as smartphones or computers, to participate in digital services.
- **Multinational banks that have a physical presence across countries could play a more proactive role in syncing up FS for migrants across major corridors.** Multinational banks can facilitate cross-border account access for migrants, allowing them to use the same bank account KYC data in both their country of origin and the destination country. This simplifies banking and reduces the need for multiple accounts. They could develop secure and user-friendly digital banking services and mobile apps that cater to the specific needs of migrants, including language options and features for cross-border transactions.

Non-governmental Organizations

- **Educate/advise on the latest technology and approaches/best practices from other contexts/use cases while advocating for citizen needs and requirements in policy.** NGOs can convene multiple organizations and governments around the world and should use this role to explore international partnerships and collaborations to learn from best practices in other countries and advocate for their adoption. From their research and understanding,

they can provide policy briefs and recommendations that translate research findings and best practices into actionable policy suggestions. Present these to government officials, policymakers, and relevant stakeholders.

- **Convene cross-sector audiences to promote collaboration and mutually beneficial solutions.** By bringing together stakeholders from various sectors, we can harness the collective expertise and resources needed to address the complex challenges associated with digital identity in today's interconnected world. This collaboration should be facilitated through a combination of conferences, partnerships, forums, and initiatives, with a focus on fostering innovation and ensuring that identity systems prioritize user needs and privacy.
- **Play a role in helping migrants navigate due diligence processes.** NGOs can help provide migrants with clear and accurate information about the due diligence requirements they need to meet, including documentation, procedures, and timelines, while also connecting migrants with resources such as legal aid organizations, community centres, and government agencies that can provide further support.
- **Support increasing access to foundational IDs or new ID issuance.** The World Bank already has an ID4D programme which focuses on promoting digital identification systems to improve development outcomes while maintaining trust and privacy (ID4D).[121] NGOs should look to utilize such programmes to help increase access to foundational IDs for those that require it while also engaging with governments to help establish new digital identity programmes in innovative ways to ensure that all global citizens receive a means to access the ever-growing number of digital services. Providing investment, technical support and education, will be key steps for the rollout of new solutions.
- **Advocate for strengthening political and commercial bilateral ties across major migration corridors.** While governments will be key to confirming these agreements, NGOs can convene the relevant parties and act as mediators for collaboration and discussions. They can gather and analyse data and research on the economic, social, and political benefits of strengthening bilateral ties in migration corridors, which can, in turn, help establish relationships with government officials and policymakers in both sending and receiving countries.

6.2 Africa

1. **Create solutions that are citizen-oriented and abide by data privacy regulations to ensure the privacy and security of individuals' data.** Governments should look to build from existing programmes in place such as existing birth registration databases and other such identity solutions. To add to this, they should also look to ensure that solutions abide by existing data privacy regulations in place but also look to amend such regulations considering international best practices such as GDPR among others. Aligning themselves to these will ensure that they have a leading perspective on data privacy and will assist when cross-border acceptance of digital ID is implemented. For example, to start, countries could begin by building upon the existing birth registration system instead of creating completely new solutions to utilize existing infrastructure, which not only helps reduce costs but also increases the likelihood of getting mass adoption due to the amount of information already known.
   Stakeholders involved: government

2. **Develop and implement a comprehensive plan to drive coordinated and united cross-sector campaigns focused on improving digital infrastructure within the country.** Although mobile internet availability has increased, Africa's internet coverage still lags behind other regions—with digital divides still an issue in remote and underserved areas in all countries. Yet, uptake is a bigger problem today than coverage. Africa's uptake gap has widened, both relative to other regions and relative to availability: while 70 percent of Africa's regional

121 https://id4d.worldbank.org/

population has availability of mobile internet, less than 25 percent are using it—resulting in an average uptake gap of almost 50 percent (The World Bank, 2021).[122] If left unaddressed, these divides will exacerbate existing income inequalities. In terms of access to formal financial systems, there is also limited availability of access points to obtain formal financial services (AFI, 2022).[123] In order to tackle the hurdle of digital literacy and, equally importantly, its usage, all key stakeholders, including the governments, regulators, financial services providers, IGOs and NGOs, must have collective efforts to sustain investments in driving coordinated or united cross-sector campaigns on improving digital literacy and digital access, as well as financial education to nurture digital inclusion.
Stakeholders involved: government

3. **Governments may need to garner greater collaboration between themselves and the private sector, enlisting organizations that will "accept" credentials for their services while also understanding other roles within the ecosystem, e.g., mobile network operators as potential identity providers.** Current digital identity solutions within Africa are limited to working predominantly in the public sector, with little collaboration yet with the private sector. However, it is here where collaboration between the sectors can provide value for all stakeholders even if the Government is the end, responsible for providing a foundation identity to people. The private sector not only provides use cases which are often accessed by citizens more frequently, ensuring the adoption of digital identity solutions, but can also provide greater learnings for the public sector on how to create a successful digital identity ecosystem that benefits all parties. Africa can leverage the AfCFTA, including different economic zones in Africa, to begin such discussions and promote acceptance. Additionally, any solution should move toward open architecture to allow transparency within the solution but also the creation of APIs for greater collaboration and use of the ecosystem.
Stakeholders involved: government and financial service organizations

Kenya

- **The government needs to be transparent about its digital identity solution and meet international privacy and data regulations.** In a statement released by Civil Society Groups, they urged the slow-down of implementation of the digital ID system and instead look to increase discussions with the public sector to ensure this initiative moves in the direction that is favourable for all parties (The Star, 2023).[124] Building this trust within the solution will enable greater adoption from both citizens using it and also private sector organizations who wish to use it during their operations to gain efficiencies. Kenya is moving at a very quick pace to develop its digital identity solution for the country. Before even considering how to be portable across borders, it must address the issues which will affect both adoption and usefulness. Furthermore, Kenya should look to implement global legal and technology standards that are commonplace to ensure that it is able to delve deeper into cross-border use and that barriers are limited. It is key that the government own this dialogue and present this openly to the public.
Stakeholders involved: government

- **Address what digital identity entails and how it can be used in other sectors (e.g., use in other sectors).** A clear challenge behind the Kenyan digital identity solution is that there is a

122 https://www.worldbank.org/en/news/feature/2021/09/24/narrowing-the-digital-divide-can-foster-inclusion-and-increase-jobs
123 https://www.afi-global.org/wp-content/uploads/2022/07/Leveraging-Digital-ID-and-e-KYC-for-the-Financial-Inclusion-of-Forcibly-Displaced-Persons-FDPs-Risks-and-Opportunities.pdf
124 https://www.the-star.co.ke/news/realtime/2023-05-19-lobby-groups-to-state-slow-down-enactment-of-digital-ids/

significant portion of the population that does not trust or completely understand the plans put in place by the government. The government need to help organizations and citizens understand what digital identity entails, and what their plans for its use both inside the public sector and in the private sector are. Gaining the trust of all stakeholders is vital to ensure that people are inclined to use it, but also to ensure the solution is able to gain maximum value. Financial service organizations also have a role to play here. They must work with the government closely to understand how the new digital identity can be utilized within its onboarding and payment processes, encouraging its customers to use the system.
Stakeholders Involved: government and Financial Service Organizations

- **Adopt paper-based and electronic systems at the same time, extend coverage in the long term, and use different means of authentication to avoid exclusion.** While Kenya is attempting to push through its digital identity solution quickly, it must first understand that systems should not be designed to exclude anyone from accessing particular services. Kenya needs to ensure that their digital identity solution can also be accessed using a paper-based solution as well for those lacking access to digital services, to ensure access for all. In the long run, they can extend the coverage as infrastructure grows in the country to increase adoption and create a uniform approach. The government need to provide such a system to ensure all solutions are protected by regulation and trusted while financial service organizations need to ensure a variety of different identification solutions can use its onboarding processes.
Stakeholders Involved: government and Financial Service Organizations.

6.3 Asia and Oceania

1. **Place a high priority on actively engaging and participating in domestic and international standardization efforts, focusing on increasing collaboration, contribution, and involvement to drive tangible progress and outcomes in standardization initiatives.** With Asia having strong digital identity programmes such as SingPass in Singapore and Aadhaar in India, there is already a strong understanding from these countries of what components are key to the success of a digital identity ecosystem. While they differ in approach, the governments of such countries should work together and within the wider global ecosystem to assist in the creation of domestic and international standards that not only provide learnings for other countries within the Asia region who have not fully realised the benefits of digital identity but also helps create approaches that make interoperability between solutions simpler. They could also play a kind of mentor role and inspire other countries by promoting their results and challenges. NGOs, as the largest inter-governmental bodies, can help convene countries and create the right infrastructure for open dialogue, discussion and collaboration to take place.
Stakeholders Involved: government and NGOs

2. **Collaborate within the region to grow understanding and develop further agreements for cross-border digital identity discussions.** While governments are key to creating common agreements and working through interoperability issues, financial services have a huge role in allowing solutions to work within their sector. Financial service organizations from Asia should look to work together both within their respective countries and within the continent to help one another understand how digital identities can be used within their operational processes. Financial service organizations from countries such as Singapore can assist others in learning what changes need to be made to accept purely digital identity credentials for onboarding, allowing for greater learning.
Stakeholders involved: financial service organizations

3. **Develop and implement a comprehensive plan to drive coordinated and united cross-sector campaigns focused on improving digital infrastructure within the countries and strong data protection laws to ensure data privacy is protected.** While in some areas of the region, huge technological successes and advancements are being made, the region's digital divide constrains productivity growth. For example, with only a quarter of the overall population using the Internet, Indonesia has one of the lowest internet penetration rates in Southeast Asia. And while access is affordable in Vietnam and Bangladesh, internet connections are often slow (IMF, 2023).[125] The right technology infrastructure for digital IDs is essential to provide security, authentication, interoperability, data integrity, scalability, privacy protection, regulatory compliance, a positive user experience, resilience, and trustworthiness in a digital identity ecosystem. It forms the foundation for the successful implementation and adoption of digital identity solutions. Governments should look to directly invest in creating the correct infrastructure within their countries while NGOs can also assist with this, helping invest in some countries where required.
Stakeholders involved: government and NGOs

Bangladesh

- **Collaborate with Other International governments.** Governments can foster international cooperation and collaboration among different countries and stakeholders. This includes sharing best practices, knowledge exchange, and joint initiatives to address the challenges associated with cross-border acceptance of digital identities. The government should look to learn from nearby countries such as Singapore and India to not only learn best practices but also begin a dialogue on how they can start accepting digital identity credentials issued from other jurisdictions.
Stakeholders Involved: government and NGOs

- **Implement the correct regulation to both Implement digital identity and protect the citizens.** Policymakers can work toward harmonizing standards and regulations related to digital identity across jurisdictions. Engagement with regional organizations, such as the South Asian Association for Regional Cooperation (SAARC), can also be valuable to harmonize standards within the South Asian region. While the government will be a key member here, the inclusion of financial services organizations will help stakeholders understand current barriers and, therefore, potential solutions that will be beneficial to all.
Stakeholders involved: government and financial services

- **Utilize the A2I programme for acceleration.** The a2i Programme in Bangladesh advocates for the establishment of international standards through collaboration with relevant international organizations, such as the International Organization for Standardization (ISO), the International Telecommunication Union (ITU), and the World Wide Web Consortium (W3C). These organizations have expertise in developing standards for digital identity management, authentication, and privacy. The a2i Programme believes that international consensus-building among governments, regulatory bodies, technology providers, industry associations, and civil society organizations is essential for setting international standards for cross-border digital identities.
Stakeholders involved: government

125 https://www.imf.org/en/Blogs/Articles/2023/01/09/asias-productivity-needs-a-boost-that-digitalization-can-provide

6.4 Europe

1. **Implement measures to enhance trust and incentivize widespread adoption of existing digital identities by the private sector.** With digital identity uptake numbers still low throughout the whole of Europe, the need to engage the private sector throughout Europe is required to encourage use and provide greater use cases. This is especially potent given the issues surrounding the changes to the e-IDAS regulations. Measures should include greater transparency in digital identity solutions while also providing greater education on digital identity across society with feedback mechanisms to help answer questions but also improve on the solution based on user and organization feedback.
   Stakeholders involved: government, financial service organizations and NGOs

2. **Place a high priority on actively engaging and participating in domestic and international standardization efforts, focusing on increasing collaboration, contribution, and involvement to drive tangible progress and outcomes in standardization initiatives.** One of the key outcomes of these new regulations is the development of mass cross-border digital identity solutions. This means that individuals across European countries will have the ability to use their digital identities seamlessly when accessing services, conducting transactions, or interacting with institutions across borders. This interoperability is a monumental step forward in simplifying and streamlining processes that were previously complex due to varying national regulations. The European initiative to create cross-border digital identity solutions has attracted significant global attention. Many other countries and regions are closely monitoring these developments as a benchmark for their own digital identity initiatives. Europe's approach could set a precedent for the establishment of standards and best practices in the digital identity space on a global scale, even if it is clear that the EU has an advantage compared to other regions in terms of integration and regional collaboration.
   Stakeholders involved: government, financial service organizations and NGOs

3. **Design a regulatory framework that protects the use of digital identities and enables organizations to use them without the risk of undue liability concerns.** One of the primary reasons for the absence of private sector engagement is liability issues, i.e., if the identification is inaccurate, it must be determined who is responsible for issuing fines/ consequences. It is key that a regulatory framework is created, with assistance from all different private sector organizations, to address such concerns. The framework should include how digital identities are created, verified, stored and used while also creating a cadence for organizations to be constantly vetted to ensure their systems abide by such regulations and information is correct and up-to-date. This will enforce trust in digital identity solutions and allow the private sector to realise the benefits that come with digital identity ecosystems. Doing this within the entire European region will also help create a standard that can be used and replicated elsewhere, helping some interoperability issues
   Stakeholders involved: government and financial service organizations.

Germany

- **Grow awareness and education to help address challenges within the country.** With some individuals and organizations being cautious about digital change, it is key for the government to help educate citizens and build relationships that transform that. Work should be done to highlight the benefits that digital identity will bring to individuals and organizations. They should also look to be as transparent as possible on the solution they create, to ensure that privacy and data concerns are addressed. A feedback mechanism will also allow changes to be made that organizations and citizens suggest, helping to create greater trust within government and digital services. Furthermore, the government will need to ensure that any solution remains inclusive and allow individuals to have a choice if they

wish to use an analogue solution as opposed to a digital one.
Stakeholders involved: government and financial service organizations.

- **Adapt technical solution for e-IDAS 2.0.** Germany's digital ID solution still requires changes to ensure that it can become compatible with the changes e-IDAS 2.0 regulation will enforce. Currently, limited smartphones support the German mobile e-ID scheme, meaning that it prohibits many citizens from accessing the solution. Additionally, its authentication approach makes it very difficult to get German e-ID data and move that to another European digital wallet. Without the flexibility to adjust this system, they will struggle to make it compliant, therefore making it difficult to allow cross-border acceptance of digital identity. The government must ensure they can adapt their current solution to future-proof it and make it accessible for all.
Stakeholders involved: governments

- **Concentrate on remittances as a use case for e-IDAS 2.0.** The current EU Digital Wallet's primary use cases are healthcare, education, payments and mobile driving licenses. This will provide learnings from all different sectors to ensure they understand the changes required to ensure that its useful for citizens. Once this is accomplished, the government and financial service providers should look to understand how onboarding can be better established using the credentials issued. The learnings will allow Germany to understand how best to onboard migrants from Europe, but also begin to understand how other such solutions outside of the EU can accomplish the same result.
Stakeholders involved: government, financial service organizations and NGOs

6.5 North and South America

1. **Stronger links are needed between regulators and the public and private sectors, while central banks must further improve their governance framework.** The public sector and national governments are key to embedding trust in digital identity, while private sector organizations provide the use cases that drive adoption. Additionally, Central banks are key institutions in ensuring the stability and integrity of financial systems. They often oversee payment systems, which are critical components of the digital economy. Strengthening the governance framework for digital identity under central bank purview can help ensure that digital identities are robust, secure, and trusted, particularly in financial transactions and provide roles for all stakeholders. With so many different jurisdictions, provinces and states that may own various aspects of individuals' identities, they must work together to understand the best approach to create a cohesive framework to allow interoperable solutions.
Stakeholders involved: government and financial service organizations.

2. **Identify viable economic corridors between countries for meaningful use cases and build trust frameworks for this.** In the United States, the largest migration corridor is observed between Mexico and the USA, with approximately 11 million Mexicans currently residing in the USA (World Migration Report, 2022).[126] This situation presents a significant opportunity to initiate a pilot programme for the utilization of digital identity solutions across these two countries, ultimately benefiting a multitude of citizens. In 2022, an estimated $54 billion was sent in remittances, making a compelling business case for governments and financial institutions to ensure that remittances are channelled through formal, secure channels, benefiting both organizations and individuals alike (Reuters, 2023).[127] By using this as an illustrative example, efforts should be directed toward identifying potential migration

126 https://worldmigrationreport.iom.int/resources/wmr-2022-worlds-largest-migration-corridors
127 https://www.reuters.com/world/americas/remittances-mexico-hit-record-strong-peso-softens-impact-2023-07-03/#:~:text=Mexican%20President%20Andres%20Manuel%20Lopez,receiving%20country%2C%20just%20behind%20India

corridors within the broader region, thereby facilitating the testing of similar technologies in the most promising locations
Stakeholders Involved: government and NGOs

3. **Identify the evolving needs of users and service providers in different cross-border scenarios and engage in bilateral and multilateral cooperation in collaboration with relevant stakeholders.** Colombia, for example, has recognized the significance of cross-border travel as a valuable use case for its digital identity system, permitting its utilization in this context. However, there is a need to extend these efforts on a larger scale. Collaborating with relevant stakeholders in bilateral and multilateral partnerships can facilitate the alignment of these systems, fostering interoperability and enabling users to access services effortlessly across international boundaries. Moreover, a thorough examination of the appropriate use cases for testing will provide deeper insights into the effectiveness of these solutions in cross-border scenarios.
Stakeholders involved: government, financial service organizations and NGOs

Colombia

- **Expand on the work done with the Colombian digital identity use across borders.** Colombia is one of the first countries globally to allow its citizens to use an updated version of their digital national identity card — known as La Cédula Digital Colombian —as a passport when travelling to eight other South American countries (NFCW, 2022).[128] While this is just for the use case of travel, it presents the opportunity for Colombia to collaborate with other South American countries to begin work on accepting their credentials across other industries as well, such as financial services. The government should look to work with other governments and private sectors to understand the requirements for this to work. Additionally, they should also look at how they can accept other credentials and what is required for this.
Stakeholders involved: government and NGOs.

- **Private and public organizations collaborate closer to collectively shape the role of the private sector within digital identity ecosystems.** It's crucial to leverage a sandbox environment for testing potential user experiences and solutions to foster interoperability and build user trust. The government should collaborate more closely with the private sector to explore the diverse ways citizens can benefit. To achieve this, the government needs to identify opportunities for streamlining processes and cutting operational expenses. By strengthening their collaboration, they can jointly offer a unified and valuable solution for the nation.
Stakeholders involved: government

- **Conduct a comprehensive assessment of Colombia's current digital infrastructure and network.** This should be done to identify areas for improvement and growth to meet the evolving needs of the country. Although there have been investments since 2000, there is still a difference in the rural and urban issues within the country. While internet access reaches around 70 percent of the population, for many going online is still too expensive and often slow (TS2, 2023).[129] The government should look to understand how to best improve this and allow many more citizens to access digital services, especially looking at ways to decrease costs and lower barriers to entry.
Stakeholders Involved: Governments

128 https://www.nfcw.com/2022/08/10/378486/colombia-to-let-citizens-use-digital-id-for-contactless-cross-border-travel-in-south-america/
129 https://ts2.space/en/internet-access-in-colombia-2/

7. Call To Action

Remittances, as noted, are a key economic driver for many. As the world becomes more connected than ever, with travel across borders becoming even more common, this is only predicted to grow. The recommendations noted above, while valuable, will take time to implement and, therefore, will take a while before value can be attributed and unlocked for the stakeholders involved. There are critical steps various stakeholders can take in the near term that will allow progress within this industry.

Governments and policymakers

Allocate resources and investments toward the ongoing development of digital identity infrastructure, focusing on enhancing its scalability, security, and interoperability. Globally, many governments have begun to develop their national digital identity schemes. The key to success, however, is to ensure clear top-level buy-in and grow adoption by the masses. Governments should develop useful solutions for use cases that create a better user experience and reduce inefficiencies. While this differs all over the World, key use cases should be identified by understanding where major pain barriers currently exist and where value can be unlocked. This can include bank account onboarding, access to digital healthcare, background checks, job onboarding and many others. Governments in developing countries should also look at expanding their digital access, especially to rural communities within countries, as a major enabler to driving the adoption of digital services and growing their digital identity solutions.

Financial service providers

Conduct a comprehensive analysis and documentation of the current challenges and difficulties associated with the use of digital identity. From the understanding gathered, many financial service providers wish to use digital identity technologies but remain hesitant due to risk and liability issues. Financial service organisations should work directly with government regulators to convey the issues that remain around the acceptance of digital identity and work jointly with the government to overcome such challenges. Financial services should also look at engaging through global organisations such as FATF to further existing guidance on digital identity, especially with regard to both portable digital identity and acceptance across borders.

Non-governmental Organizations

Collaborate with international organizations, governments, and local stakeholders to conduct thorough assessments of the existing digital infrastructure in developing countries and identify key areas that require improvement. As stated, digital identity is increasing internationally and NGOs and international development institutions such as the World Bank are assisting developing countries with the creation of digital identity solutions as they look to grow greater access to services. NGOs need to continue to push this, while also advancing the use case of cross-border payments within its work. With their understanding of the technology and expertise, they should look to further help countries learn these new technologies.

Global

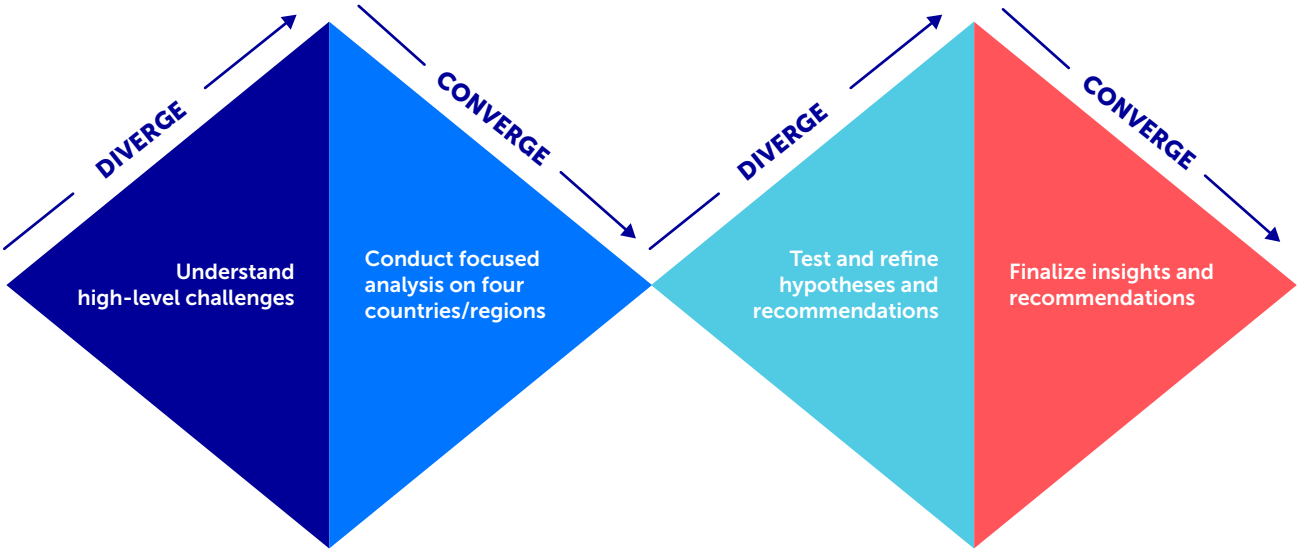
Organize regular conferences, workshops, and forums that bring together representatives from different countries to discuss and share best practices, challenges, and opportunities related to cross-border digital identity acceptance that lead to bilateral and multilateral discussions. The challenge of setting up cross-border digital ID systems cannot be solved by one country or one organisation. Governments, regulators, NGOs, and financial institutions should look to cooperate and coordinate their efforts toward a common goal and purpose. Whether an existing organisation exists today (ex G20) or if a new entity is required for this effort is still up for debate. We have yet to see all stakeholders in a global forum, but there have been discussions in such places as the Global Government Forum and OECD but just the government usually attends this. Regardless, there should be a working group to help understand the global issues that we have discussed in this report and look at what action is required to move the industry forward. An initial priority could be defining specific digital identity standards for the use case, as well as requirements from all stakeholders to help begin developments into a trust framework. Creating agreements between governments is key to advancing digital identity and a precursor for possible pilots and proofs of concept. The learnings from these will be pivotal for global advancement, helping provide greater value for organisations and, more importantly, growing financial inclusivity for migrants globally.

Appendix

Double Diamond Methodology

This research requires input from a large array of sources and information points, and a global understanding of the landscape that exists today. The double diamond methodology was employed to ensure a comprehensive understanding of the global landscape whilst also narrowing in specific case studies and use cases.

The following four steps were taken:



1 Analyse and Understanding High-Level, Global Challenges

Research was conducted into the challenges with portable digital identity by exploring pain points in a global context. To achieve this, desk research was undertaken (January-April 2023), exploring publicly available information related to digital identity, cross-border digital identity initiatives, KYC and AML regulations and migration and remittance patterns and trends. To supplement this, interviews were conducted (April-June 2023) with financial service providers, remittance service providers, governments, NGOs, and experts within this space to gain further insights from various stakeholders. Following these interviews, the initial hypotheses for challenges within this space were validated while also beginning to understand potential solutions and industry views.

2 Identify, Prioritise and Conduct Focused Analysis

Then, four countries at differing levels of economic development were selected. Using desk research, countries that met pre-defined selection criteria regarding digital identity appetite, adoption, and compliance with FATF standards were highlighted while also looking to gain global coverage of different perspectives and cultures. With the four countries chosen, it was possible to investigate further into the challenges and benefits identified.

3 Test and Refine Hypothesis and Recommendations

Following phases one and two, the project had a defined list of different hypotheses on both the challenges and benefits of the adoption of portable digital identity solutions. After understanding all the challenges identified during both the global research and interviews, the project distilled these to understand their context. Recommendations for each of the challenges were then analysed to understand what recommendations could be formulated to address the pain points. Following the creation of the analysis and recommendations, the project team tested their hypothesis with identified individuals, experts, and organizations to help refine them into actionable items.

4 Finalise Insights and Recommendations

After gathering all this information and after testing and refining the findings and recommendations, the key outcomes have been distilled down into this report. Highlighting the key challenges that currently exist today and presenting information on specific country nuances enabled the creation of recommendations for key stakeholders (governments, Financial and Remittance Service Organisations, Policymakers and NGOs) to cooperate and co-invest in specific changes that will benefit the industry, unlock value and promote greater financial inclusion for people on the move.

Glossary

Identity: Criteria that are used to describe individuals, including (but not limited to) name, date of birth, nationality, address and fingerprints (WEF, 2021).[130]

Digital Identity: A collection of individual attributes associated with a uniquely identifiable individual (e.g., name, date of birth, occupation, health status) stored and authenticated in the digital sphere and which are trusted and used for transactions, interactions, and representations online and in the digital world (WEF, 2021).[131]

Entity Resolution: Entity Resolution is a technique to identify data records in a single data source or across multiple data sources that refer to the same real-world entity and to link the records together.[132]

Identity Credentials: Issued to individuals by organisations that have verified an individual and can attest to their identity claim; additionally, identity credentials can also detail a qualification, competence or authority for an individual – examples include a passport, national identity card and driving licence (WEF, 2021).[133]

Identification: The process of establishing who an entity is within a given population or context often takes place through identity proofing, which verifies and validates presented attributes, such as name, birth date, fingerprints and iris scans (WEF, 2021).[134]

Authentication: The process of determining whether authenticators such as a fingerprint or password used to claim a digital identity are valid, i.e., that they belong to the same entity that first established that particular virtual identity (WEF, 2021).[135]

Portable Digital Identity: A portable digital identity gives users a way to re-use their verified identity credentials across multiple devices while protecting personal data. Portable identity is a way for people to prove their legal identity safely and securely to help reduce fraud, manage data sharing, and enhance privacy (Transmit).[136]

National Identity Cards: A national identity card is a portable document, typically a plasticised card with digitally embedded information, that someone is required or encouraged to carry as a means of confirming their identity (Tech Target).[137]

Know Your Customer: Anti-money laundering policies and procedures are used to determine the identity of a customer and the type of activity that is "normal and expected" and to detect activity that is "unusual" for a particular customer (Acams).[138]

Anti-Money Laundering: Anti-money laundering (AML) is a set of regulations and procedures designed to prevent, identify, and counter the concealed transfer of illicit funds (Britannica).[139]

130 https://www3.weforum.org/docs/WEF_Guide_Digital_Identity_Ecosystems_2021.pdf
131 https://www3.weforum.org/docs/WEF_Guide_Digital_Identity_Ecosystems_2021.pdf
132 https://towarddatascience.com/an-introduction-to-entity-resolution-needs-and-challenges-97fba052dde5
133 https://www3.weforum.org/docs/WEF_Guide_Digital_Identity_Ecosystems_2021.pdf
134 https://www3.weforum.org/docs/WEF_Guide_Digital_Identity_Ecosystems_2021.pdf
135 https://www3.weforum.org/docs/WEF_Guide_Digital_Identity_Ecosystems_2021.pdf
136 https://www.transmitsecurity.com/blog/portable-identity
137 https://www.techtarget.com/searchsecurity/definition/national-identity-card
138 https://www.acams.org/en/resources/aml-glossary-of-terms#k-4058d03a
139 https://www.britannica.com/money/anti-money-laundering-aml

Migrant: The UN Migration Agency, International Organisation for Migration (IOM), defines a migrant as any person who is moving or has moved across an international border or within a State away from his/her habitual place of residence (United Nations).[140]

Remittances: Money that is sent from one party to another. Any payment of an invoice or a bill can be called a remittance. Migrant remittances are commonly understood as private monetary or in-kind, cross-border and internal transfers that "migrants" send, individually or collectively, to people with whom they maintain close links (United Nations, 2015).[141]

Foundational ID: An identification system primarily created to manage identity information for the general population and provide credentials that serve as proof of identity for a wide variety of public and private sector transactions and services. Common types of foundational ID systems include civil registries, universal resident or national ID systems, and population registers (WorldBank).[142]

Functional ID: An identification system created to manage identification, authentication, and authorization for a particular service or transaction, such as voting, tax administration, social programmes and transfers, financial services, and more. Functional identity credentials—such as voter IDs, health and insurance records, tax ID numbers, ration cards, driver's licenses, etc.—may be commonly accepted as proof of identity for broader purposes outside of their original intent, particularly when there is no foundational ID system (WorldBank).[143]

140 https://www.un.org/en/fight-racism/vulnerable-groups/migrants#:~:text=Who%20is%20a%20migrant%3F,the%20person's%20legal%20status
141 https://www.un.org/en/development/desa/population/migration/events/other/workshop/2015/docs/MPP_Issue_21.pdf
142 https://id4d.worldbank.org/guide/glossary
143 https://id4d.worldbank.org/guide/glossary

Case Studies

Case Study – Africa - Kenya

Case Study – Asia and Oceania - Bangladesh

Case Study – Europe - Germany

Case Study – North and South America - Colombia

CASE STUDY

Africa - Kenya

MIGRATION AND REMITTANCE STATISTICS (Migration Data Portal, World Bank)

1.1 million
2% of population
Immigration

Major immigration corridors:

Somalia Tanzania Uganda Sudan India

535k
Emigration

Major emigration corridors:

UK USA Tanzania Uganda Canada

REMITTANCE

$4 billion - 3.6% of GDP
Inflows

$8.9 million
Outflows

KENYA CONTEXT, IDENTITY AND DIGITAL IDENTITY

- Historically, Kenyans have been using M-PESA as their main choice for remittance payment – 96 of households use it (Vodafone).
- A key issue surrounding sending remittances to Kenya is the cost - averaged at 8.45 percent.
- This is a mobile money solution that works by customers firstly registering at small retailers, often mobile phone stores – this is where identity verification takes place. To obtain a sim card, KYC is undertaken where personal identifiable information is required, and checks are done.
- Once registered, the M-PESA user can deposit cash in exchange for electronic money and this can be sent to friends and family within Kenya and now in other African countries too – as well as other money transfer organisations.
- In 2019, there was an amendment to the Registration of Persons Act to enable Kenya to establish a National Integrated Identity Management System which was referred to as Huduma Namba. The aim of this was to centralize all existing identity systems, making them interoperable – however, following a ruling in 2021, the High Court of Kenya ruled that the rollout of a country-wide biometric ID scheme was illegal due to data privacy risks.
- In 2023, it announced to investigate creating a new secure digital ID system that links up all the country's databases and enables safe and seamless access to a wide range of government and private sector services – including KYC.
- A large section of the population still does not have full access to internet connectivity – with penetration around 33 percent which will negatively impact any digital identity adoption.

CHALLENGES

Lack the proper safeguards for security of personal data

This is pegged on Kenya's lack of robust security infrastructure to protect sensitive information and maintain data privacy.

Lack of private sector collaboration with digital identity

While the private sector engages with the government on several aspects, there has been a lack of collaboration around digital identity for Kenya.

Lack of internet connectivity will always harness adoption

In January 2023, there were 17.86 million internet users in Kenya. However, this means that 67.3 percent of the population remained offline.

RECOMMENDATIONS

1. **Government needs to be transparent about its digital identity solution and meet international privacy and data regulations.** Building this trust within the solution will enable greater adoption from both citizens and organizations.

2. **Address what digital identity entails and how it can be used in other sectors (e.g., use in other sector).** The government need to help citizens and organizations understand its use in society to foster adoption.

3. **Adopt paper-based and electronic systems at the same time, extend coverage in long-term, use different means of authentication to avoid exclusion.** Solutions must not leave any individual or group excluded.

CASE STUDY

Asia and Oceania - Bangladesh

MIGRATION AND REMITTANCE STATISTICS (Migration Data Portal, World Bank)

2.1 million
1.3% of population
Immigration

7.4 million
Emigration

Major immigration corridors:

Major emigration corridors:

REMITTANCE

$21.5 billion - 4.6% of GDP
Inflows

$136.8 million
Outflows

BANGLADESH CONTEXT, IDENTITY AND DIGITAL IDENTITY

- Bangladesh has established a national identity system which has over 80 percent of the population registered which is a key enabler for a digital identity programme. The National Identity Card (NID) is a unique document that is issued to citizens of Bangladesh and used as the primary identification document. It is used in various contexts, including for government services, financial transactions, and voting
- The government of Bangladesh has introduced the "Digital NID" or "Smart NID" to enhance its functionality and useability - Citizens can use it in both the private and public sector with around 33 organizations and departments accepting it.
- In 2020, the Bangladesh Financial Intelligence Unit issued guidance for electronic Know Your Customer (e-KYC), which enables any bank or financial service provider (FSP) to open a bank account or digital wallet with the customer taking pictures of the front and back of their NID card and submitting it alongside a selfie. The bank or FSP then verifies the NID and profile photo against the national election commission database automatically to open the customer account.
- However, there remain many challenges that prohibit individuals from being able to access formal remittance channels, with more than 60 percent of the population not owning a bank account.
- Additionally, internet penetration only stands at 38.9 percent explaining how the digital infrastructure within Bangladesh is yet to hit the mainstream.

CHALLENGES

Large technology infrastructure issues limits success

Bangladesh's internet penetration rate stood at 31.5 percent of the total population at the start of 2022. Lack of Awareness and Education.

Trust and security concerns with digital identity solutions

In Bangladesh, recent surveys have suggested that trust in the Bangladesh government is declining, especially with many saying it declined heavily during the pandemic.

No unified effort for one digital identity

In recent years there has been various approaches by different government and private sector entities.

RECOMMENDATIONS

1. **Collaborate with other international governments.** Governments can foster international cooperation and collaboration among different countries and stakeholders

2. **Implement the correct regulation to both implement digital identity and protect the citizens.** Policymakers can work toward harmonizing standards and regulations related to digital identity across jurisdictions.

3. **Utilize the A2I Programme for Acceleration.** The a2i Programme believes that international consensus-building among governments, regulatory bodies, technology providers, industry associations, and civil society organizations is essential for setting international standards for cross-border digital identities.

CASE STUDY

Europe - Germany

MIGRATION AND REMITTANCE STATISTICS (Migration Data Portal, World Bank)

15.8 million
18.8% of population
Immigration

3.9 million
Emigration

Major immigration corridors:

Major emigration corridors:

REMITTANCE

$19.3 billion - 0.5% of GDP
Inflows

$25.6 billion
Outflows

GERMANY CONTEXT, IDENTITY AND DIGITAL IDENTITY

- Since the 1900s, the government has issued identity cards to its residents.
- Since 2010, the identity card has become an electronic ID card. The expectation was for e-ID to become the core identification means for citizens in both the public and private sectors but this has yet to accomplish this objective thus far - only 6 percent of German citizens actively made use of the card's electronic function.
- The German population are notoriously very privacy aware, and more reluctant to share information online.
- There is a fear by some that it gives too much power to the government to access citizens' information and data, with many citing data protection regulations as a reason for not using it
- There has not been a large uptake in its use in the private sector. This is down to a few reasons such as the difficulty in integrating digital identity solutions within organisations and a question as to the value it would bring internally.

CHALLENGES

Issues with current German digital ID solutions and its compatibility

The current German Digital ID solution does not have the capabilities required by e-IDAS 2.0 and will require improvements.

Lack of awareness and education

Despite the growing prevalence of digitalization, a notable proportion of users in the country continue to favour traditional analogue procedures over their digital counterparts

Slower to digitalization than other EU countries

Only 50 percent of Germans possess basic digital skills – compared to 80 percent of Finnish citizens.

RECOMMENDATIONS

1. **Grow awareness and education to help address challenges within the country.** With some individuals and organizations being cautious to digital change, it is key for the government to help educate citizens and build relationships that transform that.
2. **Adapt technical solution for e-IDAS 2.0.** Germany's digital ID solution still requires changes to ensure that it can become compatible with the changes e-IDAS 2.0 regulation.
3. **Concentrate on remittances as a use case for e-IDAS 2.0.** Government and financial service providers should look to understand how onboarding can be better established using the EU digital wallet for migrants.

CASE STUDY

North and South America - Colombia

MIGRATION AND REMITTANCE STATISTICS (Migration Data Portal, World Bank)

1.9 million
3.7% of population
Immigration

Major immigration corridors:

3 million
Emigration

Major emigration corridors:

REMITTANCE

$9.4 billion - 2.7% of GDP
Inflows

$419 million
Outflows

COLOMBIA CONTEXT, IDENTITY AND DIGITAL IDENTITY

- While Colombians have had national identity cards since the 1950s, they implemented a digital identity equivalent at the end of 2020.
- The goal of this was a new electronic and digital ID to provide a high level of assurance in digital public services - This has stemmed from a large digital transformation programme that the government is undergoing, with positive opportunities coming because of its fast implementation.
- The new digital identity is available for individuals to store on their mobile phone, enabling both online authentication via utilizing biometrics and in person verification through a dedicated verification facility.
- While originally a tool for use for access in the public sector, the government have been attempting to sign up private sector organizations - In 2023, the government began various pilots of facial authentication with several banks where customers can perform remote transactions through a home computer or mobile, with facial biometrics compared to their national digital ID.
- In addition to the government developing a digital identity solution, three of the main banks within Colombia have come together to develop Soy Yo. This enables individuals who have onboarded onto bank accounts to be able to access other services at other organizations without having to prove identity again.
- The banks, Davivienda, Bancolombia and Banco de Bogotá, first devised an initial pilot study that looked at streamlining the onboarding of users to multiple services, increasing user convenience by consolidation of services in a single app, while at the same time reducing costs for the participating companies.

CHALLENGES

Lack of adoption

Currently, there is not large amounts of services available with digital identity

Minimal private-public collaboration decreases valuable use cases

Despite the growing prevalence of digitalization, a notable proportion of users in the country continue to favour traditional analogue procedures over their digital counterparts

Technical infrastructure still lagging behind

Despite investments since 2000, there is still a gap between rural and urban areas within the country

RECOMMENDATIONS

1. **Extend efforts to promote the use of Colombian digital identities across borders.** The government should look to create additional use cases for cross border use.
2. **Private and public organizations to collaborate closer to collectively shape the role of the private sector within digital identity ecosystems.** The government needs to identify opportunities for streamlining processes and cutting operational expenses.
3. **Conduct a comprehensive assessment of Colombia's current digital infrastructure.** Internet use in Colombia for many is too slow and inefficient.

List Of References

1. McKinsey, Olivia White, 2019, https://www.mckinsey.com/capabilities/mckinsey-digital/our-insights/digital-identification-a-key-to-inclusive-growth
2. Allied Market Research, Pramod B, Monica C, Vineet K, 2022, https://www.alliedmarketresearch.com/remittance-market
3. Identification for development, World Bank, 2022 https://id4d.worldbank.org/global-dataset
4. World Bank, 2022, https://remittanceprices.worldbank.org/sites/default/files/rpw_main_report_and_annex_q422_final.pdf
5. United Nations, https://www.un.org/sustainabledevelopment/health/#:~:text=Goal percent203 percent20targets,-3.1 percent20By percent202030andtext=3.3 percent20By percent202030 percent2C percent20end percent20the,diseases percent20and percent20other percent20communicable percent20diseases.
6. KNOMAD, Dilip Ratha, Sonia Plaza, Eung Ju Kim, Vandana Chandra, Nyasha Kurasha, and Baran Pradhan 2023, https://www.knomad.org/publication/migration-and-development-brief-38
7. United Nations, Department of Economic and Social Affairs, https://www.un.org/en/desa/much-more- percentE2 percent80 percent98lifeline percentE2 percent80 percent99-millions-households-remittances-can-spur-global-growth-says
8. Mckinsey, Olivia White, Anu Madgavkar, James Manyika, Deepa Mahajan, 2019 https://www.mckinsey.com/capabilities/mckinsey-digital/our-insights/digital-identification-a-key-to-inclusive-growth
9. Identification for development, World Bank, https://id4d.worldbank.org/guide/mutual-recognition-ids-across-borders-0#:~:text=When percent20IDs percent20issued percent20by percent20one, promote percent20safe percent20and percent20orderly percent20migration.
10. IISD, Rohan, 2022, https://sdg.iisd.org/commentary/generation-2030/leveraging-digital-identity-for-greater-financial-and-social-inclusion/
11. United Nations, https://www.unodc.org/roseap/en/sustainable-development-goals.html#:~:text=Target percent2016.9 percent20 percent2D percent20By percent202030 percent2C percent20provide,national percent20legislation percent20and percent20international percent20agreements.
12. UN Refugee Agency, Nannie Skold, 2021, https://www.unhcr.org/neu/70493-unhcr-strengthens-efforts-on-digital-identity-for-refugees-with-estonian-support.html
13. Joseph Rowntree Foundation, Lavinia Mitton, 2008, https://www.jrf.org.uk/sites/default/files/jrf/migrated/files/2234.pdf
14. FATF, 2023, https://www.fatf-gafi.org/media/fatf/documents/recommendations/pdfs/Guidance-on-Digital-Identity-Executive-Summary.pdf
15. FATF, 2013, https://www.fatf-gafi.org/content/dam/fatf-gafi/guidance/Opportunities-Challenges-of-New-Technologies-for-AML-CFT.pdf.coredownload.pdf
16. Council of EU, 2022, https://www.consilium.europa.eu/en/press/press-releases/2022/12/06/european-digital-identity-eid-council-adopts-its-position-on-a-new-regulation-for-a-digital-wallet-at-eu-level/
17. LexisNexis, 2023, https://risk.lexisnexis.com/global/en/insights-resources/research/true-cost-of-financial-crime-compliance-study-global-report
18. European Parliament, Susanna Tenhunen, 2022, https://www.europarl.europa.eu/RegData/etudes/BRIE/2022/699491/EPRS_BRI(2022)699491_EN.pdf
19. Forbes, Frederic Ho, 2021, https://www.forbes.com/sites/jumio/2021/05/03/how-national-digital-ids-benefit-both-citizens-and-businesses/
20. Forbes, David G.W. Birch,2021, https://www.forbes.com/sites/davidbirch/2021/09/16/digital-identity-should-be-a-big-business-for-banks/
21. Forbes, Federic Ho, 2021, https://www.forbes.com/sites/jumio/2021/05/03/how-national-digital-ids-benefit-both-citizens-and-businesses/
22. Wiley Online Library, Shirin Madon, 2021 https://onlinelibrary.wiley.com/doi/full/10.1111/isj.12353
23. IFRC, 2022 https://www.ifrc.org/sites/default/files/2021-12/Digital-Identity percentE2 percent80 percent93An-Analysis-for-the-Humanitarian-Sector-Final.pdf
24. UIDAI, https://uidai.gov.in/en/
25. BankID, https://www.bankid.com/
26. World Bank, Julia Clark, Anna Diofasi and Claire Casher, 2023 https://blogs.worldbank.org/digital-development/850-million-people-globally-dont-have-id-why-matters-and-what-we-can-do-about
27. Smart Africa, 2020, https://smartafrica.org/wp-content/uploads/2020/12/BLUEPRINT-SMART-AFRICA-ALLIANCE--DIGITAL-IDENTITY-LayoutY.pdf
28. Identification for Development, https://id4d.worldbank.org/guide/mutual-recognition-ids-across-borders-0
29. Envoy Global, Jessie Butchley, 2023, https://resources.envoyglobal.com/global-news-alerts/kenya-introduction-of-biometric-e-passport/
30. Biometric Update, Stephen Mayhew, 2015, https://www.biometricupdate.com/201512/distribution-of-ecowas-biometric-id-cards-to-begin-in-january-2016
31. World Bank, 2020 https://documents1.worldbank.org/curated/en/261151588384951057/pdf/Benin-Burkina-Faso-Togo-and-Niger-Second-Phase-of-West-Africa-Unique-Identification-for-Regional-Integration-and-Inclusion-WURI-Project.pdf
32. AFDB, 2023 https://www.afdb.org/en/news-and-events/press-releases/west-african-monetary-institute-receive-

8-million-african-development-fund-support-enhanced-banking-identification-and-financial-sector-efficiency-west-african-monetary-zone-6030
33. AFDB, Sheila Okiro, 2023, https://www.afdb.org/en/documents/multinational-west-african-monetary-institute-wamz-unique-bank-identification-ubi-and-digital-interoperability-project-appraisal-report
34. African Union, https://au.int/sites/default/files/documents/38507-doc-dts-english.pdf
35. Biometric Update, Frank Hersey, 2022, https://www.biometricupdate.com/202202/id4d-report-2022-to-see-significant-progress-toward-paradigm-shift-in-digital-id
36. Relief Web, 2023, https://reliefweb.int/report/burkina-faso/togo-benin-burkina-faso-and-niger-join-west-africa-regional-identification
37. World Bank, Lucia Hanmer, 2017 https://medium.com/world-of-opportunity/opening-doors-how-national-ids-empower-women-cross-border-traders-in-east-africa-8443c98e2aad
38. Ecowas, 2019, https://ecowas.int/ecowas-to-conduct-sensitization-on-national-biometric-identity-card-and-the-fight-against-trafficking-in-persons/#:~:text=The percent20ENBIC percent20which percent20will percent20improve,Ghana percent2C percent20Senegal percent20and percent20Guinea percent20Bissau.
39. Biometric Update, Frank Hersey, 2021 https://www.biometricupdate.com/202109/mastercard-partnership-to-capture-biometrics-of-30-million-africans
40. Biometric Update, Frank Hersey, 2022 https://www.biometricupdate.com/202212/mastercard-africa-digital-id-scheme-to-benefit-from-50m-of-dfc-funding-to-its-partners
41. Mastercard, 2023 https://www.mastercard.com/content/dam/public/mastercardcom/na/global-site/public-sector/other/humanitarian-community-pass-january2023.pdf
42. International Telecommunication Union, 2021, https://www.itu.int/en/ITU-D/Statistics/Documents/facts/FactsFigures2021.pdf
43. ODPC, https://www.odpc.go.ke/dpa-act/
44. Cipesa, Juliet Nanfuka, 2022 Vodafone, https://www.vodafone.com/about-vodafone/what-we-do/consumer-products-and-services/m-pesa
45. Vodafone, https://www.vodafone.com/about-vodafone/what-we-do/consumer-products-and-services/m-pesa
46. 3 News, Laud Nartey, 2021 https://3news.com/kenya-court-declares-biometric-id-rollout-illegal/
47. Biometric Update, Ayang Macdonald, 2023 https://www.biometricupdate.com/202305/kenya-unveils-details-on-new-digital-id-rollout-india-potential-partner
48. Datare Portal, Simon Kemp, 2023, https://datareportal.com/reports/digital-2023-kenya
49. MOSIP, https://mosip.io/
50. ASEAN, https://asean.org/wp-content/uploads/2020/12/Adopted-ASEAN-Digital-Integration-Framework.pdf
51. ASEAN Briefing, Alexander Chipman Koty, 2022 https://www.aseanbriefing.com/news/thailand-and-singapore-sign-agreements-to-deepen-economic-cooperation/
52. Philippine News Agency, Raymond Carl Dela Cruz, 2023 https://www.pna.gov.ph/articles/1192927
53. MTI, 2023 https://www.mti.gov.sg/Newsroom/Press-Releases/2023/01/Factsheet-on-Frameworks-on-Cooperation-in-Digital-Economy-and-Green-Economy
54. DFAT, https://www.dfat.gov.au/trade/agreements/in-force/anzcerta/Pages/australia-new-zealand-closer-economic-relations-trade-agreement#:~:text=The percent20agenda percent20was percent20endorsed percent20at,can percent20operate percent20across percent20the percent20Tasman.
55. DFAT, https://www.dfat.gov.au/trade/services-and-digital-trade/australia-and-singapore-digital-economy-agreement
56. GOV.UK, 2021 https://www.gov.uk/government/publications/memoranda-of-understanding-with-singapore-digital-trade-facilitation-digital-identity-and-cyber-security/memorandum-of-understanding-on-digital-identities-cooperation
57. MTI, https://www.mti.gov.sg/-/media/MTI/Microsites/DEAs/EUSDP/EU-SGP-Digital-Partnership.pdf
58. Government Technology Agency, 2021 https://www.tech.gov.sg/files/media/media-releases/Media percent20Factsheet percent20on percent20Singpass percent20(National percent20Digital percent20Identity)_28 percent20October percent202021.pdf
59. MAS, 2022 https://www.mas.gov.sg/-/media/mas-media-library/regulation/circulars/amld/circular---non-face-to-face-customer-due-diligence-measures-1.pdf
60. Canadian Bankers Association, 2018, https://cba.ca/Assets/CBA/Documents/Files/Article percent20Category/PDF/paper-2018-embracing-digital-id-in-canada-en.pdf
61. The Economic Times, Preeti Motiani, 2018 https://economictimes.indiatimes.com/wealth/personal-finance-news/who-are-eligible-to-apply-for-aadhaar-find-out/articleshow/59998036.cms?from=mdr
62. Cronfa Swan, Umar Bashir, Arpan K. Kar, https://cronfa.swan.ac.uk/Record/cronfa53060/Download/53060__16145__30bafc2d109c485089258f5cac663025.pdf
63. National News, PBNS, 2022, https://newsonair.com/2022/01/04/aadhaar-going-global-the-potential-point/
64. Christian Science Monitor, Riddhima Dave, 2022 Biometric IDs: India is a 'laboratory for the rest of the world ..., https://www.csmonitor.com/World/Asia-South-Central/2022/0425/On-biometric-IDs-India-is-a-laboratory-for-the-rest-of-the-world.
65. Philippine Identification System, 2022 https://psa.gov.ph/content/72-million-filipinos-now-registered-philsys
66. MOSIP, Suraksha P, 2022 https://mosip.io/news-events/identifying-a-billion
67. Neda, https://neda.gov.ph/philsys/
68. Biometric Update, Chris Burt, 2023 https://www.biometricupdate.com/202302/australia-and-state-govts-agree-on-digital-id-credential-sharing-deal

69. Biometric Update, Ayang Macdonald, 2022 https://www.biometricupdate.com/202207/xydus-mastercard-gain-digital-id-trust-accreditations-in-uk-Australia
70. Digital.Govt.NZ, 2022 https://www.digital.govt.nz/digital-government/programmes-and-projects/digital-identity-programme/problems-benefits-and-outcomes/
71. New Zealand Parliament, 2023 https://bills.parliament.nz/v/6/b00cd25e-18dd-48d7-a68a-047aa9f41fce?Tab=history
72. Singapore government Development Portal, https://www.developer.tech.gov.sg/our-digital-journey/digital-government-exchange/files/DGX percent20DIWG percent202022 percent20Report percent20v1.5.pdf
73. Biometric Update, Frank Hersey, 2021, https://www.biometricupdate.com/202111/cross-border-digital-id-is-coming-mastercard-plans-to-supply-infrastructure
74. European Commission, 2023, https://ec.europa.eu/commission/presscorner/detail/en/ip_23_467
75. Asian Development Bank, 2017 https://www.adb.org/publications/asia-infrastructure-needs
76. Brookings, 2020 https://www.brookings.edu/wp-content/uploads/2020/12/Development-Southeast-Asia-Ch2-Digital.pdf
77. DataRePortal, Simon Kemp, 2022 https://datareportal.com/reports/digital-2022-bangladesh
78. Utilities One, 2023 https://utilitiesone.com/telecommunications-infrastructure-and-the-future-of-digital-identities
79. NorthSouth University, http://www.northsouth.edu/newassets/files/ppg-research/PPG_5th_Batch/1._MahadiCitizensTrustin_Public_Institutions_Exploring_Trust_in_Public_Officials_in_Bangladesh.pdf
80. The Daily Star, Azfar Adib, 2021 https://www.thedailystar.net/views/opinion/news/time-make-digital-identity-nationwide-reality-2919206
81. European Commission, 2023 https://digital-strategy.ec.europa.eu/en/policies/eidas-regulation
82. Ukraine Now, https://ukraine.ua/invest-trade/digitalization/
83. Dig Watch, 2021 https://dig.watch/updates/spain-and-germany-will-test-cross-border-digital-identity
84. In Cyber News, Fabrice Deblock, 2022 https://incyber.org/en/digital-identity-toward-age-of-reason/
85. Its Me, https://www.itsme-id.com/en-BE/why-itsme/security
86. European Commission, 2019 https://commission.europa.eu/strategy-and-policy/priorities-2019-2024/europe-fit-digital-age/european-digital-identity_en
87. Knomad,2022 https://www.knomad.org/sites/default/files/2022-11/migration_and_development_brief_37_nov_2022.pdf
88. Biometric Update, Ayang Macdonald, 2023 https://www.biometricupdate.com/202306/eu-financial-associations-want-traditional-payments-excluded-from-eidas-regulation
89. Tech Monitor, Afiq Fitri, 2022 https://techmonitor.ai/focus/the-state-of-digital-identity-in-europe
90. CEIC, https://www.ceicdata.com/en/germany/telecommunication/de-internet-users-individuals--of-population#:~:text=Germany percent20DE percent3A percent20Internet percent20Users percent3A percent20Individuals percent3A percent20 percent25 percent20of percent20Population percent20data,to percent202021 percent2C percent20with percent2032 percent20observations.
91. IDnow, Heinrich Grave, 2023, https://www.idnow.io/blog/digital-identity-index-2023-study-future-germany/#:~:text=Our percent20Digital percent20Identity percent20Index percent202023,the percent20existence percent20of percent20digital percent20services.
92. CEPA, Laura Kabelka, 2022 https://cepa.org/article/deutsche-katastrophe-germany-fights-digital-backwardness/
93. European Commission, 2023 https://digital-strategy.ec.europa.eu/en
94. NFCW, Tom Phillips, 2022 https://www.nfcw.com/2022/08/10/378486/colombia-to-let-citizens-use-digital-id-for-contactless-cross-border-travel-in-south-america/
95. Identification for Development, https://id4d.worldbank.org/guide/mutual-recognition-ids-across-borders-0#:~:text=In percent20Latin percent20America percent2C percent20for percent20example,and percent20Uganda percent20in percent20East percent20Africa.
96. KPMG, 2022 https://kpmg.com/xx/en/home/insights/2022/07/flash-alert-2022-135.html
97. Government of Canada, 2023 https://www.canada.ca/en/innovation-science-economic-development/news/2021/11/government-of-canada-announces-partnership-with-the-european-commission-to-examine-the-use-of-digital-credentials.html
98. Digital Policy Alert, 2021 https://digitalpolicyalert.org/change/1330-digital-identity-requirements-in-uk-canada-agile-nations-digital-credentials-project
99. Thales Group https://www.thalesgroup.com/en/markets/digital-identity-and-security/government/mobile-driver-licence
100. Trulioo, 2020 https://www.trulioo.com/blog/identity-verification/business-mexico
101. Open Identity Exchange, Rob Laurence and Ewan Willars, 2020 https://canada-ca.github.io/PCTF-CCP/docs/RelatedPolicies/Blueprint-for-National-International-Oversight-of-the-Digital-Identity-Market-March-2020.pdf
102. DIACC, 2022 https://diacc.ca/voila-verified/#:~:text=A percent20Voil percentC3 percentA0 percent20Verified percent20Trustmark percent20signals,meet percent20international percent20standards percent20and percent20regulations.
103. DGX, 2022 https://www.tech.gov.sg/files/media/corporate-publications/FY2021/dgx_2021_digital_identity_in_response_to_covid-19.pdf
104. GOV.UK, 2022 https://www.gov.uk/government/publications/agile-nations-progress-report-2020-to-2022/agile-nations-2020-2022-progress-report#digital-credentials-and-digital-trust-services
105. GOV.UK, https://www.gov.uk/government/groups/agile-nations

106. Apple, 2021 https://www.apple.com/newsroom/2021/09/apple-announces-first-states-to-adopt-drivers-licenses-and-state-ids-in-wallet/#:~:text= percentE2 percent80 percent9CThe percent20addition percent20of percent20driver percent27s percent20licenses,Apple percent20Pay percent20and percent20Apple percent20Wallet.
107. Identification for development, https://id4d.worldbank.org/guide/mutual-recognition-ids-across-borders-0
108. NFCW, Tom Phillips, 2022 https://www.nfcw.com/2022/11/10/380218/brazil-begins-rollout-of-contactless-mobile-identity-cards/#:~:text=Residents percent20of percent20six percent20Brazilian percent20states,travel percent20to percent20other percent20South percent20American
109. Forbes, Lincoln Ando, 2021 https://www.forbes.com/sites/forbestechcouncil/2021/06/02/understanding-the-significance-of-digital-identification-problems-in-latin-america/?sh=1c025e74525f
110. Identification for Development, https://id4d.worldbank.org/
111. World Bank, 2021 https://www.worldbank.org/en/news/feature/2021/09/24/narrowing-the-digital-divide-can-foster-inclusion-and-increase-jobs
112. Alliance for Financial Inclusion, Anshul Pachouri, Thomas Murayi Maina, Vedika Tibrewala and Venkat Goli, 2022 https://www.afi-global.org/wp-content/uploads/2022/07/Leveraging-Digital-ID-and-e-KYC-for-the-Financial-Inclusion-of-Forcibly-Displaced-Persons-FDPs-Risks-and-Opportunities.pdf
113. STAR, Lindwe Danflow, 2023 https://www.the-star.co.ke/news/realtime/2023-05-19-lobby-groups-to-state-slow-down-enactment-of-digital-ids/
114. IMF, https://www.imf.org/en/Blogs/Articles/2023/01/09/asias-productivity-needs-a-boost-that-digitalization-can-provide
115. UN Migration, 2021 https://worldmigrationreport.iom.int/resources/wmr-2022-worlds-largest-migration-corridors
116. Reuters, Kylie Madry, 2023 https://www.reuters.com/world/americas/remittances-mexico-hit-record-strong-peso-softens-impact-2023-07-03/#:~:text=Mexican percent20President percent20Andres percent20Manuel percent20Lopez,receiving percent20country percent2C percent20just percent20behind percent20India
117. TS2, Marcin Frackiewicz, 2023 https://ts2.space/en/internet-access-in-colombia-2/
118. World Economic Forum, Derek O'Halloran, Manju George, Cristian I. Duda, 2021 https://www3.weforum.org/docs/WEF_Guide_Digital_Identity_Ecosystems_2021.pdf
119. Toward Data Science, Sonal Goyal, 2021 https://towarddatascience.com/an-introduction-to-entity-resolution-needs-and-challenges-97fba052dde5
120. Transmit Security, Alex Brown, 2022 https://www.transmitsecurity.com/blog/portable-identity
121. Tech Target, Katie Terrell Hanna, 2023 https://www.techtarget.com/searchsecurity/definition/national-identity-card
122. ACAMS, https://www.acams.org/en/resources/aml-glossary-of-terms#k-4058d03a
123. Britannica, https://www.britannica.com/money/anti-money-laundering-aml
124. United Nations, https://www.un.org/en/fight-racism/vulnerable-groups/migrants#:~:text=Who percent20is percent20a percent20migrant percent3F,the percent20person's percent20legal percent20status
125. United Nations, https://www.un.org/en/development/desa/population/migration/events/other/workshop/2015/docs/MPP_Issue_21.pdf
126. Identification for development, https://id4d.worldbank.org/guide/glossary
127. Migration Data Portal, https://www.migrationdataportal.org/

List of Organizations Consulted

#	Organization/ Independent Expert
1	Accenture
2	Accenture
3	Airtel Group
4	Bank for International Settlements
5	Bank of England
6	Bill and Melinda Gates Foundation
7	Calp Network
8	Canada government - DIAAC
9	CommUnique
10	FATF
11	FinTech for International Development
12	GMSA
13	HSBC
14	IAMTN
15	IFRC
16	Intesa Sanpaolo
17	Mastercard
18	Mastercard
19	Merchantrade Asia
20	nChain
21	OIX
22	Remitly
23	Ripple
24	Ropes and Gray LLP
25	Singapore Gov
26	SWIFT
27	The World Bank
28	Tony Blair Institute
29	Virgin Money
30	Western Union
31	WISE
32	M-Pesa
33	African Development Bank Group
34	Bangladesh government - Ministry of Home Affairs
35	Deutsche Bank
36	IDNow
37	Soy Yo
38	Abdourazakhe LAMINOU ABANI (WURI)
39	Bruno Moreau (DI Expertise)
40	David Birch (DI Expertise)
41	Ali Hussein Kassim - Kenyan Expert
42	Julie Zollmann (Kenya Payments Expert)

ABOUT THE UNITED NATIONS CAPITAL DEVELOPMENT FUND

UNCDF mobilizes and catalyzes an increase in capital flows for SDG impactful investments to Member States, especially Least Developed Countries, contributing to sustainable economic growth and equitable prosperity.

In partnership with UN entities and development partners, UNCDF delivers scalable, blended finance solutions to drive systemic change, pave the way for commercial finance, and contribute to the SDGs. We support market development by enabling entities to access finance in high-risk environments by deploying financial instruments, mechanisms and advisory.

ABOUT MIGRATION AND REMITTANCES

UNCDF aims to improve the functioning of remittance markets by improving the financial resilience of men and women in migrant workers' families while supporting economic development in countries of origin and destination. To strengthen the global evidence, UNCDF collects, analyses, and disseminates reliable and comparable remittance transactions as well as survey data. UNCDF engages with public and private sector stakeholders to strengthen the capacity of regulators to contribute to the design of migrant-centred financial products and services such as savings, credit, insurance, payment services, remittances, pensions, and investments.

Contact

migrantmoney@uncdf.org

Visit

migrantmoney.uncdf.org

UNCDF

UNCDF