Evaluation report for e-KYC pilot in Bangladesh

24th December, 2019

MSC MicroSave Consulting | www.microsave.net

a2i innovate for all 2041

Cabinet Division
Government of the People's Republic of Bangladesh

ICT DIVISION
FUTURE IS HERE

UNDP
Empowered lives. Resilient nations.

Contents

1. Project background and objectives

Project background and objectives

The lack of documentation was a critical barrier to accessing financial services, cited by 26% of unbanked people in low-income countries as per the World Bank's 2017 Global Findex Survey. The marginalized segments of society show greater evidence of this barrier. The survey also estimated that less than half of all adults in the poorest 40% of households have a bank account and approximately 375 million unbanked adults in developing countries who comprise 18% of the global population are constrained by not having the necessary documentation.

While many developing countries are in the process of building robust foundational ID systems, a growing number of developing countries that have such infrastructure already in place are either implementing e-KYC or developing regulations to support its use. Opening financial accounts and registration of SIM cards have been some of the early use-cases of digital IDs that many nations have utilized for digital inclusion. Countries such as India have been very successful in using digital ID infrastructure in augmenting financial inclusion.

The current Know Your Customer (KYC) process in Bangladesh requires customers of financial service providers to manually fill in an extensive 12-page paper-based form, provide their photo identification credentials, and enter their signature (specifically the case for mobile financial service providers), nominee details, and other additional documentation. This paper-based KYC is therefore costly to collect, transfer, process, and store. In addition, the country has been facing challenges as a result of a large number of fake accounts or identities that have come into existence to get extra benefits or hide correct information.

The high cost of customer onboarding owing to paper-based KYC has been a significant deterrent to financial inclusion in Bangladesh. As it stands, onboarding bottom-of-the-pyramid customers and maintaining their bank accounts is a loss-making business for financial service providers. Transactions made by account holders are typically low in terms of both volumes and value. As a result, these accounts have been classified as low-risk accounts and there is a need to devise low-cost onboarding and maintenance for low-risk accounts.

An alternate KYC mechanism has to be devised to address these issues. This new KYC mechanism is expected to lead to the easier inclusion of unbanked and marginalized to the formal financial services ecosystem. With this objective, Bangladesh government decided to set up a working group with representation from key stakeholders in the financial services ecosystem.

The working group on e-KYC was formed in 2016, with participation from Bangladesh Bank, National Identity & Registration Wing, Access to Information (a2i), Bangladesh Telecommunication Regulatory Commission, and other financial institutions in the country. Its objective is to lay down detailed strategy and guidelines to propagate e-KYC in the country. The decision to form this working group was under the advice of access to information (a2i), which was earlier under the Prime Minister's Office and is now a part of the ICT division of the Government of Bangladesh.

After detailed deliberations, the working group conceived the draft guidelines and protocols for e-KYC pilot in a bid to simplify the account opening process and reducing the time taken down to a few minutes. The group also proposed that customer

identification be performed with a one-to-one[1] match, two-factor authentication involving National ID (NID) and fingerprints and live photographs, using a mobile application or web-based portal. The NID database under the jurisdiction of the Election Commission was the reference database against which matching was undertaken.

A pilot was executed under the directions of the Bangladesh Financial Intelligence Unit (BFIU) and the Financial Inclusion Department of Bangladesh Bank. Its objective was to test the new processes, protocols, and assess the capacity of financial institutions to implement the new process. A target of opening 1,500 bank accounts was set for the 19 participating financial institutions across 22 districts and 50 locations in Bangladesh. Four categories of accounts were opened. These were 10 Taka accounts, Social Safety Net (SSN) accounts, Mobile Financial Services (MFS) accounts, and garment worker accounts. Two techniques of e-KYC were used—fingerprint authentication and face matching or Optical Character Recognition (OCR).

The pilot was conducted from 25th September to 3rd October, 2019. Access to Information (a2i) assigned the responsibility of pilot evaluation to MicroSave Consulting (MSC). The objective of this project was to:

- Evaluate the pilot and capture the advantages and drawbacks of the e-KYC processes.
- Assess customers' needs and feedback and understand problems faced by financial institutions in administering the process.
- The scope of work also included providing recommendations on the future implementation process, suggesting amendments to draft e-KYC guidelines and recommendations that Bangladesh Bank had already prepared and circulated among key stakeholders.

[1] In one to one matching biometric data captured on device is matched against the biometric data stored in NID database against that particular NID number.

2. Approach and methodology

Approach and methodology

Our approach was to conduct in-depth, semi-structured, qualitative interviews with key stakeholders including customers. The objective was to understand their lived experiences with the new e-KYC processes. We conducted the evaluation after the pilot completed. However, the MSC team visited a couple of sites during the pilot period to understand the processes for both fingerprint and face-matching modes in detail. After that, the team prepared research guides for the participating financial institutions, the customers who opened accounts during the pilot, the technology provider of the facial recognition software—Giga Tech, and Bangladesh Bank.

We conducted telephonic interviews, lasting 20 to 30 minutes approximately with e-KYC nodal officers and other officers who were on-site administering the e-KYC process during pilot execution. We conducted an independent study through a qualitative discussion tool developed by our internal behavioral researchers. With guidance from a2i, we selected seven financial institutions to participate in the research and covered different segments, that is, 10 Taka, SSN, MFS and Garment workers. In addition, we covered both forms of authentication—fingerprint and face-matching.

We conducted interviews with bank officials around four major thematic areas:

- Communication and outreach to the target segment
- Authentication success rates, time required
- Technical and functional problems encountered during the pilot process
- The overall perception of financial institutions

After interacting with the bankers, the team visited one pilot site for five of the seven selected financial service institutions. We conducted in-depth interviews with eight to ten customers at each site. The financial institutions were instructed to invite only those customers who had opened their accounts through e-KYC.

We conducted interviews with customers around four major thematic areas:

- Understanding their socio-economic profile
- Their experience of the account-opening process which included both pain-points and positive feedback
- Understanding how they would like to utilize their newly opened accounts
- The overall perception of the new e-KYC process as against the old paper-based KYC process

Our team also interacted with Bangladesh Bank, to understand the regulators' point of view with respect to what the expectations of the pilot were and how the e-KYC ecosystem evolved. We also got an overview of the existing concerns and the measures Bangladesh Bank aims to take to ensure a robust e-KYC ecosystem in the country. From the technology perspective, we interacted with technology stakeholder Giga Tech, the architect of the OCR/face-matching technology for the pilot, who helped us gain a better understanding of the processes.

Note: Owing to operational hurdles, Dutch Bangla Bank and Sonali Bank could not arrange e-KYC customers for MSC to interact with. However, given our in-depth interactions with other bank customers that cover a wide sample spread across urban, semi-urban, and rural geographies, we believe that it should not affect the findings presented in this study. The specific supply-side challenges that bank stakeholders within Dutch Bangla Bank and Sonali Bank faced are already a part of the report.

3. Lessons from interactions with financial institutions

Lessons from interactions with financial institutions

As stated in the earlier section, the first task that the team undertook was to understand the processes involved with the two modes of e-KYC. The following section describes the processes so that the lessons can be contextualized.

Fingerprint based e-KYC verification process

01 Potential customer brings NID card with himself or herself to the site of bank account opening.

02 Bank official opens its customer onboarding mobile application, keys in the 13 digit NID number of potential customer and date of birth as provided in the NID card.

03 Impression of thumb and index finger of both hands is captured through a biometric device.

04 The NID card number, date of birth and biometric of four fingers captured are sent for verification to the Election Commission (NID) server.

05 There is instantaneous response from the NID server and there are two possible responses - biometric match found and no biometric match found. If match found then further details are filled to open account (move to step 6). If match not found, then step 1 to 4 are repeated.

06 Eight data fields are keyed in. In case the banking channel is Agent banking then move to Step 7 else move to Step 8.

07 Impression of thumb and index finger of both hands is captured through a biometric device. This is for bank records and enable biometric based banking services through agents.

08 Account category is selected i.e. 10 Taka account/ Social Safety net account/ Garment workers account/ Mobile Financial Services account

Money is deposited by the customer based on his or her discretion

09

10

Account is activated (in-principle as of now, as there are no regulations of e-KYC from Bangladesh bank) and paper-based details are filled out.

Face-matching and optical character recognition (OCR) based e-KYC process

01

Customer brings the NID card with them to the site of bank account opening. They can bring either the NID in original or a clear color photocopy.

02

The bank official opens the web-based customer onboarding application. During the pilot, most banks who used face-matching technology used this application.

03

Both front page and back sides of the NID card are scanned and uploaded on to the web application. The application automatically fetches the data fields from the scan through OCR technology. The data fields are the NID number, date of birth, name in English, name in Bengali, father's name in Bengali, mother's name in Bengali and present address in Bengali. The present address field appears in Bengali as given in the NID card.

04

Additionally, some data fields are keyed in, that is, profession, mobile number, gender, permanent address, nominee and relation with nominee. All the fields here are entered in English.

05

Live photograph of potential customer's face is taken.

06

All details captured in step 3, 4, and 5 appear in a single page of the web application, which is then pushed to the Election Commission's database for verification of all the text fields, scan of NID and live picture

At the backend, the bank cues the verification request. The Giga Tech system queries the Election Commission's database by sending the NID and date of birth of the applicant to the server.

07

08

Based on guidelines by Bangladesh Financial Intelligence Unit (BFIU), if the score for biometric match falls below the minimum percentage, the bank is obliged to reject the verification process.

In case of failure, the bank reinitiates the process from step 3

09

10

The customer deposits money at their discretion.

The account is activated. As of now, the activation is in-principle, as regulations from Bangladesh Bank around e-KYC are yet to come into effect. In parallel, paper-based details required to activate the account as per the current process are filled out.

11

3.1 Findings on communication and outreach to the target segment

- Most financial institutions interviewed did not face any hurdles while reaching out to potential customers and during opening their accounts in the pilot phase. The mobilization process received support from agent banking points and union digital centers. In addition, most of them already had the community's trust, as social safety payments or cash-out services were in place. In the case of garment workers, the bankers approached the employers to get accounts opened in bulk at the factories.

- Despite the pilot being carried out in short notice, Giga Tech had issued a user manual to all the headquarters of the participating banks. Its objective was to help bank officials understand the OCR authentication process. The manual also clearly defined the quality requirements of the photos taken. Furthermore, during the pilot phase, the company had set up a call center to help solve field issues. Due to a lack of time, Giga Tech could not effectively communicate much of the information to the stakeholders who were conducting the e-KYC on the field. This then led to various process-related issues, such as poor picture quality and poor understanding of the manual.

- Public sector banks or financial institutions that lack prior experience in agent banking or MFS have faced problems in reaching out to bottom-of-the-pyramid customers. They lacked any prior product offerings or

community relationships that could be leveraged. Most of their business is carried out through brick and mortar branches at district and sub-district regions, and is urban in nature.

- For MFS and 10 Taka accounts, outreach was not done appropriately for some financial institutions. While the requirements for eligibility in the case of SSN accounts and garment workers were clear, there was inadequate clarity on whom could be targeted for 10 Taka accounts and MFS accounts. Affluent citizens, who already have multiple bank accounts, are digitally literate and have minimum utility for these accounts were targeted in some cases.

- Our findings revealed that financial institutions had enrolled e-KYC customers to other banking products as well. For example, customers walking in to open 10 TK accounts were also made to open a normal savings bank account.

- We observed that communication around the exact documents that customers needed to bring in and their format—whether in original form or as photocopy—was lacking. Some customers, especially those who opted for the face-matching mode of e-KYC, had to be sent back. The reasons for rejection were that either they had brought a black and white photocopy or their face was unclear.

- Communication on the utility of accounts being opened and what it could be used for was deficient in some cases. For instance, in some cases, customers thought that their SSN accounts were meant for depositing money alone, and no withdrawal was possible.

3.2 Findings on authentication success rates and time required

- Most financial institutions that used the fingerprint authentication mode reported that on average, it took them 5 to 7 minutes to go from Step 2 to Step 9 of the process flow described earlier.

- As per field interactions, more than 90% of the customers had successful fingerprint authentications in their first attempt.

- Aged customers and those who engaged in heavy physical labor encountered multiple authentication failures due to changes in their fingerprint from the time they had first received their NID.

- Most financial institutions that used face-matching mode for e-KYC reported that on average, it took their customers 8 to 10 minutes to go from Step 2 to Step 9 of the process flow described earlier. The reasons behind failed instances of authentication are poor technical knowledge of bank officials with regard to the process, picture quality, and connectivity.

- Approximately 80% of the customers who opted for eKYC through face-matching could authenticate themselves successfully in the first two attempts. The statistics are based on interactions with bank field officials.

- A few authentications have failed due to old NID cards, which could not be processed through OCR, or in the case of customers who were carrying poor quality photocopies of their NID cards.

Note: The findings on the time taken for successful authentication are based on in-depth interviews with bank officers and customers. Furthermore, MSC has also not seen firsthand the backend processes at Giga Tech for face matching e-KYC authentication. Our technical knowledge is based on detailed discussions with key personnel at Giga Tech.

3.3 Findings on technical and functional problems or risks

The following section describes problems with the fingerprint mode, followed by the problems with the face-matching mode.

3.3.1 Problems or risks with fingerprint-based e-KYC

- Respondents reported that the fingerprint-based e-KYC process was more stable and easier to execute compared to face-matching based e-KYC.

- Aged, infirm people or people involved in heavy manual labor found it difficult to authenticate themselves. Respondents reported a few cases where the account opening process failed. No exception handling mechanisms were in place as of the time of writing.

- Approximately eight data fields need to be filled in manually to complete the customer e-KYC form. This could lead to errors creeping in as agent banking and UDC outlets may have literacy constraints.

- Nominee details are not captured extensively as a part of the e-KYC process, as merely collecting the name and relation with nominee does not suffice. In case of a claim, the financial institution will lack adequate information to validate the nominee. We must note that Bangladesh Bank did not provide a guideline regarding the validation or verification of the nominee information.

- Financial institutions that provide agent banking services need to capture the fingerprint twice—firstly for verification against the NID server and secondly for storing the data to enable fingerprint-based agent banking services. This has both risk and cost implications.

- There are risks involved because once fingerprint-based e-KYC is rolled out, it will be both a financial and identity information. Storing it across different servers makes it prone to cybersecurity attacks with multiple points of failure. It is costly because all financial institutions that provide agent banking services need to invest heavily in the storage, security, and firewall needs of the fingerprint data. Any case of identity theft or financial fraud can severely dent customer confidence and act as a formidable deterrent to financial inclusion.

- Financial institutions have procured hardware and software independently and have obtained permission from Bangladesh Bank to use their hardware and software for the pilot. This again is a security hazard as different vendors may use different levels or techniques to ensure the security of the data stored and backed up. When implemented at a full scale, it will be difficult for the regulator to ensure all software and hardware are protected, regularly audited, and scanned for cybersecurity threats.

- Some process deviations were also observed, which is a result of independent software being procured by different financial institutions. For instance, one financial institution reported scanning the fingerprint of only both thumbs to reduce the time of account opening. In case it was successful, it did not obtain the fingerprint of index fingers. Similarly, another financial institution reported having provisions for one finger, two fingers, four fingers, and ten fingers as well. They claimed that this helps in exception handling in cases where a customer and has lost some fingers from some accident.

3.3.2 Problems or risks with face-matching based e-KYC

- Face-matching and the OCR technique was reported to have multiple issues at the start of the pilot. One reason why the fingerprint mode was smoother to implement than face-matching was the awareness of financial service providers about the process itself. Most financial institutions in Bangladesh have been using fingerprints to enable agent banking, so they had a better know-how of it as opposed to face-matching.

- Many methodical issues were reported:

  - Improper practice of capturing NID photo, which led to unwanted light being reflected from the room ceiling on the NID card plastic lamination.
  - The over-cautious practice of capturing NID or smart card photo, where agents tried to crop the NID or smart card photo led to operational issues as the system was already capable of automatic cropping of the NID or smart card. There were cases where agents tried to crop the photo by their hand and mistakenly cropped one or more important portions.
  - Network error or inconsistent network between the bank server and EC server for some banks also led to the failure of this technology.
  - The newly issued smart cards have a hologram. In some cases, photocopies of smart cards have left a white spot occurring due to reflection from the hologram. Due to this, the OCR failed to read the scan properly, which led to a textual mismatch.
  - The agents did not properly capture the applicant photo. There were cases where agents either wrongly captured the applicant's photo by cropping out parts of the applicant's face or captured the applicant's photo in very low light, resulting in a facial mismatch.

- For customers at the bottom of the pyramid, maintenance of the NID card in proper condition is a challenge. In some cases, the original NID cards were old and in a dilapidated condition, which made it difficult for the OCR software to read.

- There were confusions over what quality of devices should be used for scanning. While some used mobiles and tabs, some used office scanners. The poor quality of NID photocopies, coupled with poor quality of scanning equipment was one reason for the OCR failing to read the scans.

- Prescribed standards on camera quality and standard best practices or guidelines for image capture are absent for the financial service providers. This led to authentication failures and

multiple attempts, as for some cases the image capture was done in low light conditions or in poor angles.

- We did not find the presence of a beard to be a deterrent to image matching. However, in some cases, a woman's *hijab* had led to a dark reflection in the image, leading to an authentication failure.

- Some financial institutions have reported significant delays in getting a response from the NID server on whether the match has been successful or not. For some cases, it was instant, while for some it has taken up to two days as they had to queue up of verification requests in the election commission server.

- Financial service providers are ambiguous with respect to the exact percentage of textual and image match for authentication to be successful. Certain anomalies were observed. A person with a higher percentage of textual and image match often received an authentication failed status, while a person with a lower percentage of image and textual match received a pass.

- Adequate information is not taken with regard to nominee details. The nominee information provided as of now is not verifiable in case a claim arises.

- The protocols for obtaining customer signature are unclear. For instance, in the case of MFS providers, a manual signature is taken on mobile screen, in which case there is a high chance of signature mismatch as the target population has low levels of digital literacy and overall literacy levels are also poor.

3.3.3 Findings on the overall perception of the financial institutions

- In spite of a few problems encountered during the pilot, it was successfully executed and all financial institutions, systems designed seem capable of executing the e-KYC processes. With minor improvements (many of which have been discussed above), the e-KYC can be scaled up at the national level.

- All financial institutions we interacted with were extremely supportive of the e-KYC pilot. They were convinced that moving from paper-based KYC to electronic KYC would drastically reduce the time and cost of customer onboarding and enhance security. In addition, it would enhance the overall ease of onboarding for both the financial institutions and customers.

- As it stands, just applying for a new account under the paper-based KYC process requires filling up of 12 pages, eight signatures, and approximately 40 minutes' time. However, the proposed e-KYC process, both face-matching and fingerprint-based, brings down the entire process to just 11 fields on a digital form. The proposed process involves one signature and needs approximately 10 minutes' time.

- Typically, for customers from the bottom of the pyramid, accounts are opened at agent banking outlets. All the application documents, copies of supporting documents then have to be couriered to the designated branch. The designated branch then needs to verify the documents and account is activated. The whole process takes more than a week. Moreover, the bank

bears the transportation and storage cost of so many documents. With e-KYC, there would be no additional cost of transportation and storage, while the account activation would be almost real-time once Bangladesh Bank regulations are in place.

- At present, the e-KYC mechanism is a yes/no mode of authentication wherein the response from NID does not fetch any data apart from an authentication pass or fail status. The financial institutions could benefit if additional data from NID can be fetched into the system, especially for fingerprint-based e-KYC, as many fields need to be filled in manually. Additionally, some financial institutions requested if NID could be linked with the risk profile of a customer wherein the potential customers' creditworthiness or risk exposure could be gauged.

3.3.4 Key findings from interactions with e-KYC customers

- We solely interviewed customers who opened an account on e-KYC days through either fingerprint or face-matching technique. For most of these customers, it was the first bank account. Most of them said that they did not earn enough, hence could not save, and therefore had never felt the need to approach banks.

- We have interviewed a total of 48 customers. Approximately, 70% of the customers are engaged in cash-intensive sectors, that is, agriculture labor, garment workers, domestic help, or hotel staff, among other professions, and have a yearly income lesser than 25,000 BDT.
- Approximately 30% of customers interviewed were economically well off and engaged in large-scale trade, working as medical practitioners, students, etc. The criteria for targeting customers under 10 TK and MFS were not clear to the financial institutions, hence customers who were not from the bottom of the pyramid were targeted.

- There were marked differences in the e-KYC process narrated by different customers from different banks. Some claimed that multiple passport-size photographs were taken from them during the face-matching process. Some claimed that black and white photocopies were accepted for face-matching, others said that either original NID or colored photocopy was accepted. For fingerprint-based e-KYC also there were differences reported in the number of fingers for whom fingerprints were taken. The same narratives were checked with the financial institutions as well. They confirmed that there is a further need for process standardization.

- For most customers interviewed, it was their first bank account opening experience, so they did not have a reference to compare with. They did not have any complaints about the process per se.

- Customers who opened an account through fingerprint e-KYC mostly reported that authentication was successful for them in the first attempt and the processes pertaining to fingerprint were over in 5 to 7 minutes.

- Customers who opened an account through face-matching had different experiences depending upon their NID condition (new or old) if they were carrying it in originals or photocopies. For many, there were issues with both

NID scan and live image capture. Most reported success in one attempt only but the time taken was between 10 to 15 minutes.

- Customers who had prior experience of account opening appreciated the new process. They claimed that the earlier application process in entirety would last for 3 to 4 hours, as it would involve filling up a long-form involving multiple signatures, and submission of various documents. In contrast, the current process is under 10 minutes and requires only the NID card.

- Most customers considered fingerprint-based e-KYC to be absolutely safe, as no one could withdraw their money without their personal consent and presence. Even for face matching, they believed that it was completely safe as their NID card details and live images were being captured.

- Some customers interviewed were confused about the process, as they were made to open a basic savings bank accounts or were convinced to avail other banking products. This was most common in the case of 10 TK accounts, as there were no set criteria for the kind of customers who should be targeted for 10TK. The financial institutions that had mobilized customers for the pilot purpose leveraged to sell other offerings from the bank as well.

- Only one among the 48 customers had used the bank account for depositing 100 Taka. No other customer was found to be using the account. Financial literacy levels of the customers were found to be very poor. They had vague ideas about why the accounts were being opened. SSN customers were aware that in future social safety and government-related payments would come into their account. Moreover, garment workers assumed that any kind of government assistance would come into the account being opened.

- There were many misconceptions about the accounts being opened. Some believed that amount can only be deposited and saved and no withdrawal was possible. Meanwhile, others had mistrust that banks could use that money and invest in some other product of theirs. Some had a bad experience with financial institutions, as they were deceived by chit funds or local NGOs who took away their savings. In totality, most customers did not know how they could use the account apart from savings.

- There was confusion over whether withdrawals can be made from newly opened accounts and also on the amount that can be deposited. Even the financial institution representatives were unsure of withdrawal norms and whether the accounts had been activated

4. Recommendations

Recommendations

The recommendations are in line with the problems and risks identified through interactions with financial institutions and customers.

4.1 General recommendations

- All financial institutions in Bangladesh need to be aware of the importance of e-KYC in promoting financial inclusion. They also need to be aware of the utilities of special accounts like 10 TK and SSN, so that they can, in turn, promote financial literacy initiatives. This can encourage the unbanked and under-banked to come into the mainstream financial services market.

- The section below lists the suggestions for effective financial literacy initiatives:

  a. Build a basic version of the financial literacy module into the school curriculum. It can be a standalone subject or integrated into subjects like Mathematics and Economics.
  b. Create educational games and comic books to better understand simple concepts of financial literacy and remove the fear of banking. For example, using games like Monopoly, Mann Deshi Foundation in India has been spreading effective financial literacy among rural women. Furthermore, the Reserve Bank of India has also created characters like "Money Kumar" to promote financial literacy in a fun way under its Project Financial Literacy.
  c. Utilize the Self Help Group network to hold literacy camps.
  d. Encourage readymade garment factories to run monthly financial literacy campaigns.
  e. Provide an incentive to bank account holders if they regularly access their accounts.
  f. Provide an incentive structure to private banks to hold financial literacy campaigns for identified geographies and segments.

- Customer-centricity is of utmost importance. The target customers here are predominantly new to mainstream financial services, and financial institutions should refrain from overselling. Moreover, considerations around data security should be assigned prime importance. Before delving into operational issues, it is extremely important that the IT architecture or design and customer consent framework are thought through. The recommendations pertaining to architecture and consent framework should be materialized through an international benchmarking or best practices study along with a diagnostic study of the current ecosystem.

- The Election Commission (EC) of Bangladesh is an independent constitutional body and has many responsibilities. Hence, it may be unsuitable for the role of digital identity management agency. A separate government body needs to be carved out, which would be responsible for legislations and for defining processes, standards, and specifications and ensure safe storage of all digital identity-related data. Use cases of digital identity will evolve and have potential to form an important backbone of growing digital economy of

Bangladesh. A separate agency will be better suited to evolve digital identity as a public good infrastructure.

- A consent or data privacy framework needs to be developed so that the vulnerable and marginalized people who are new to the financial services ecosystem are not subjected to exploitation or financial fraud.

- From an operational point of view, stringent processes need to be defined and software should be aligned to collect nominee details, which can be further verified in case of a claim.

- For MFS providers, there is a need for major security enhancement. Presently, it is possible that the NID of one person can be linked with the mobile number of another person and an account can be operated. This is a security hazard and can become a source of fraudulent transactions or money laundering. However, a rigorous e-KYC in place can ensure that the NID and mobile number are unique to a person and that no other person can use the MFS account.

- The process of obtaining a manual signature from customers, should also be defined. As we mostly deal with bottom-of-the-pyramid customers, manual signature requirements can be relaxed as there is a chance of subsequent authentication mismatch.

- Outreach mechanisms need to be thought through for public sector financial institutions that traditionally have relied on a branch or brick and mortar banking model. Some partnerships may have to be fostered with private entities or district-level entities so that they can connect with the bottom-of-pyramid customers.

- The deposit and withdrawal limits need to be prescribed clearly. Standard operating procedures need to be drafted to clearly indicate account activation timelines and restrictions on deposits as well as withdrawals.

4.2 Recommendations for fingerprint-based e-KYC

- In the case of biometric data, financial services institutions that provide agent banking services presently store data in their own servers. This results in increased cost for storage and security for the individual institutions. Moreover, it makes the ecosystem vulnerable with multiple points of failure, which can be prone to cybersecurity attacks and result in incidences of identity theft or financial fraud. Storing the data on servers is also contradictory to good e-governance guidelines that specifically lay down an identity architecture with a single source of truth. Ideally, a central government authority should exist that would store and maintain all the data from a citizen's birth to death in a secure and centralized repository, as is the case of *Aadhaar* in India. No private entity should be allowed to store any biometric data.

- From an operational point of view, while the process must remain device-agnostic—specific software and hardware standards need to be prescribed for fingerprint-based e-KYC. Streamlining software and hardware specifications will automatically lead to process standardization. Specifically, the use of public devices must be tested and registered in a

centralized laboratory that will then be given a unique identifier. This serves the purpose of allowing the device to be traceable so that its functions can be analyzed and fraudulent practices managed, should they occur.

- Moreover, e-KYC data is sensitive and must be protected by stringent privacy guidelines. To this effect, each of the registered devices must not be permitted to store any biometric data and must capture the citizens' biometrics in an encrypted form to dissuade any wrongful practices. A definite guideline or SOP needs to be drafted and circulated among concerned stakeholders to further standardized processes. A document on best practices to ensure lesser authentication failures can be a value add. Closed room workshops could also be conducted to ensure better dissemination.

- Exception handling guidelines and aligned software specifications also need to be introduced for people whose fingerprints are damaged or not clear. There should be no denial of service due to fingerprint authentication failures.

- Manual data entry in the authentication process needs to be further minimized. As of now, the financial service provider fills eight fields manually in the application, which may lead to erroneous data. NID must capture within its central data repository key citizen information pertaining to identity, address, and mobile number, among others to be able to pass on the data to the screen automatically and authenticate both proof of identity and proof of address. Based on the nature of the authentication requirement, the database can validate the input parameters against the data stored and return a digitally signed "Yes" or "No" authentication response, or a digitally signed e-KYC authentication response with encrypted e-KYC data alongside other details, which would eliminate human intervention.

4.3 Recommendations for face-matching and OCR based e-KYC

- In the case of the face-matching technique, security risks need to be assessed from an architecture point of view. Ideally, all the customer details can be shared but the NID number should be masked and then shared with the financial service providers. Here too, devices must be registered and data must be encrypted to avoid ill practices.

- Despite Giga Tech sharing guidelines for minimum hardware requirements for camera and minimum photo quality requirements with the banks, the percolation of information to the field level was poor. Better training of field officials must be carried out to eliminate such issues to make the technology more effective.

- Financial service providers are confused over the exact process flow and best practices they should follow. Bangladesh Bank in association with Giga Tech should come up with standard operating procedures to be followed for face-matching, citing things to avoid thus ensuring higher authentication success. This should also include clear instructions on scanning the NID properly and techniques for live photographs to ensure better quality.

5.Annexures

Annexures

5.1 Customer Respondent Profile

- The qualitative study was spread across 5 districts with varying distance from the capital city of Dhaka.
- In-depth interviews were conducted with 48 e-KYC account holders to understand their user experience.
- Figure 1 depicts the gender profile of respondents covered in the research. Of the total sample 40% interviewed are men who are involved in different kinds of professions, that is, garment workers, domestic help while some are social safety net beneficiaries like widows, elderly, etc.
- Figure 2 shows the geographical profile of the sample covered.
- Financial literacy levels are quite low compounded by a cash-based economy and lack of accurate information regarding banking facilities.
- Monthly household expenditure of respondents ranges from BDT 8000 ($95) to BDT 15000 ($177). Their income is above the international poverty line of $1.90 per person per day. Based on their declared income the respondents are earning approximately $3 per day.
- Figure 3 depicts the various occupations the respondents are engaged in.
- Figure 4 shows the break-up of respondents stepping into formal banking services for the very first time to those who are very familiar with the same due to business ventures.

Fig 1: Gender profiles of respondents (N=48)

Fig 2: Geographical profile of respondents (N=27)

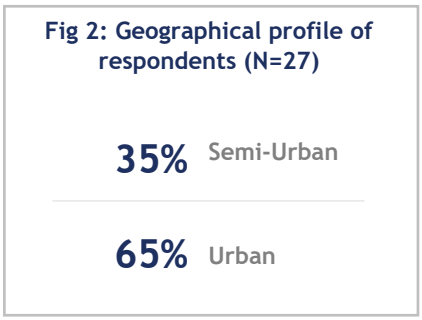


Figure 3: Occupation profile of respondents (N= 48)

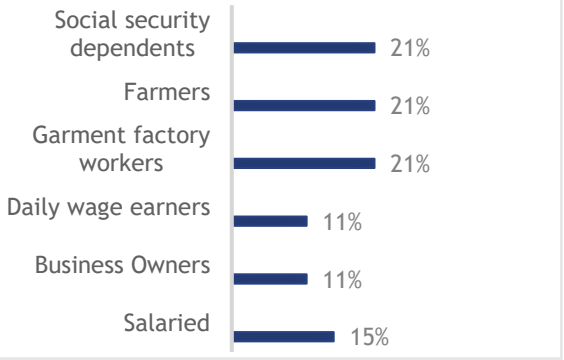
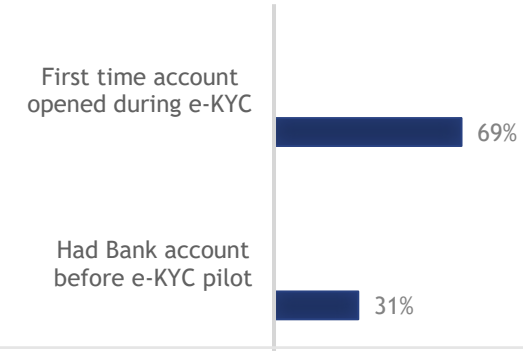


Figure 4: Level of engagement with formal banking (N= 48)



5.2 Giga Tech e-KYC verification and result timing data summary of the pilot

- Face matching verification time (as per super admin analytics of the GIGA e-KYC)
    - Average time for verification is 11.5 second/per account (with EC data response time)
    - Average time for verification is 6.5 - 8.5 second/per account (without EC response time)
- Full process completion (as per super admin analytics of the GIGA e-KYC)

(Image capture + Verification + Additional info input + any additional time taken by agent during the process + account open)

- Average time including all process is 3.5 minutes
- Category-wise:
    - Below 1 minute: 46
    - Below 5 minutes: 463
    - Below 15 minutes: 110

Exception cases:

- 30 minutes: 28 (network error/EC delay)
- 1 hour +: 57 (network error/EC delay)
- 2 day: 8 (network error/Election Commission server delay)

Data source: Giga Tech

5.3 List of financial institutions who were interviewed

Bank name	Type of authentication	Type of account
Sonali Bank	Fingerprint	10 TK Account
BRAC Bank	Face-matching	Garment Workers
United Commercial Bank	Fingerprint	10 TK account
City Bank	Face-matching	10 TK account
One Bank	Face-matching	Mobile Financial Services
Dutch Bangla Bank	Face-matching	Mobile Financial Services
NRB Commercial Bank	Fingerprint	Social Safety Net account

About Access to Information

Access to Information or a2i, a whole-of-government program of ICT Division, supported by Cabinet Division and UNDP, catalyses citizen-friendly public service innovations simplifying government and bringing it closer to people. The primary goal is to ensure easy, affordable and reliable access to quality public services for all citizens of Bangladesh.

About UNDP

UNDP works in about 170 countries and territories, helping to achieve the eradication of poverty and the reduction of inequalities and exclusion. It helps countries to develop policies, leadership skills, partnering abilities, institutional capabilities and build resilience to sustain development results. Since 1972, UNDP and its partners have helped Bangladesh make critical advances in the areas of governance, poverty reduction, climate change, and disaster resilience.

About MicroSave

MicroSave is a leading international consulting firm that offers practical, market-led solutions in the areas of digital financial services, inclusive finance, and banking, micro, small and medium enterprises, and private sector development. We focus on enhancing access to financial services to the low- and middle-income segments.

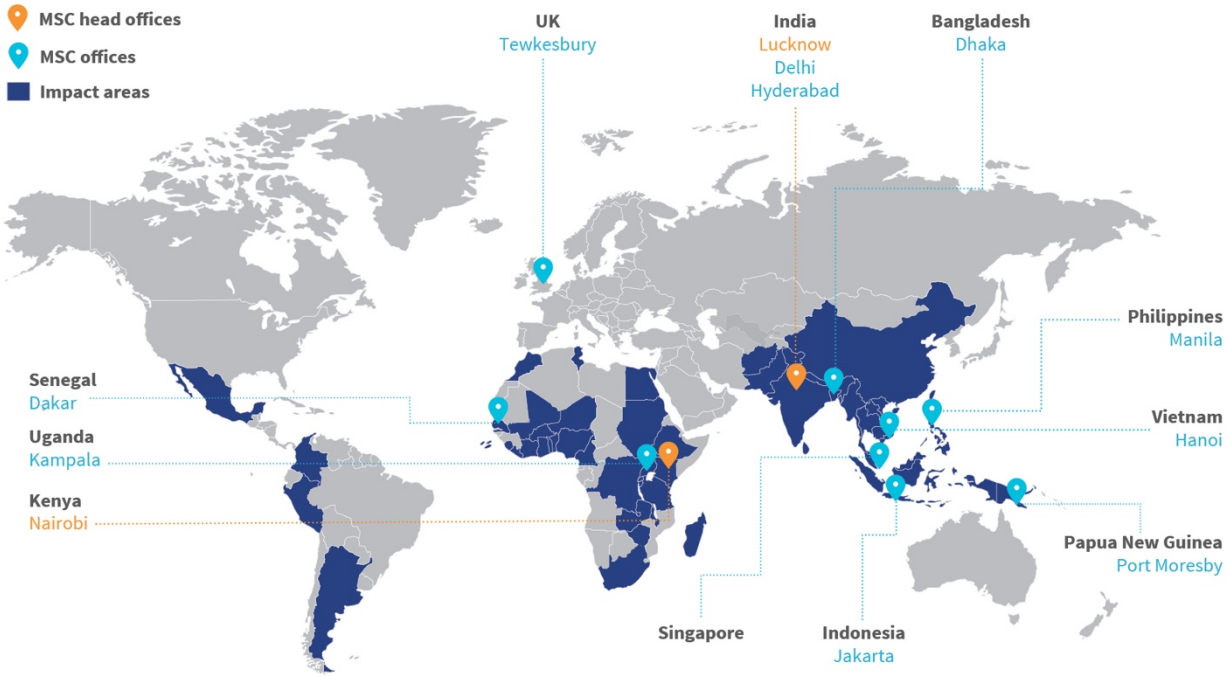
Our vision is to live in a world where everyone has access to high-quality, affordable, market-led financial services and support. For 20 years, we have worked with our clients as a locally based, international consulting firm. We have guided policy and facilitated partnerships to develop enabling ecosystems.

For further information, contact:

Mitul Thapliyal at mitul@microsave.net

Venkat Goli at venkat.goli@microsave.net

MSC
MicroSave Consulting



Asia head office

28/35, Ground Floor, Princeton Business Park, 16 Ashok Marg,
Lucknow, Uttar Pradesh, India 226001
Tel : +91-522-228-8783 | Fax : +91-522-406-3773
Email : manoj@microsave.net

Africa head office

Shelter Afrique House, Mamlaka Road, P.O. Box 76436,
Yaya 00508, Nairobi, Kenya
Tel : +25-420-272-4801 | Fax : +25-420-272-0133
Email : anup@microsave.net

www.microsave.net