REGIONAL FRAMEWORK ON ELECTRONIC KNOW YOUR CUSTOMER (E-KYC) AND ELECTRONIC IDENTITY (E-ID) FOR ECAPI

FRAMEWORK

CONTENTS

ACKNOWLEDGMENTS

This regional policy framework was developed by AFI members and endorsed by its ECAPI EGFIP as a policy guide to facilitate in-country inancial inclusion policy implementation across the AFI network in EECA and beyond. Development of this regional policy framework was partially funded by UK aid from the UK government.

INTRODUCTION

The AFI Eastern Europe and Central Asia Policy Initiative (ECAPI) supports and develops financial inclusion policies and regulatory frameworks for AFI member institutions in the Eastern Europe and Central Asia (EECA) region.

One of the key challenges to financial inclusion in many regions is the lack of legal identity; this has been addressed to an extent with the issuance of a national ID. There is now a growing body of evidence for the use of a digital ID with an ecosystem that can address some of the more nuanced challenges facing AFI members in ECAPI.

AFI Experts Group on Financial Inclusion Policy (EGFIP) in ECAPI has agreed to develop a regional policy framework to address the challenges in the region identified above. The regional policy framework is intended to:

1. Examine the policies and practices on e-ID and e-KYC in the region, and their ecosystem
2. Devise principles incorporating international standards and best practices on the implementation and use of e-ID and e-KYC

The principles proposed in this framework are drawn based on an extensive review of existing practices and policies in the region, experiences shared by AFI member institutions in ECAPI, and international best practices on e-ID and e-KYC. These guiding principles have no binding force. They have been developed to support member institutions in their implementation of e-KYC and e-ID in the region.

THE POINTS BELOW HIGHLIGHT THE KEY CHALLENGES EXPRESSED BY THE COUNTRIES IN THE REGION AND BRIEFLY SUMMARIZE THE POTENTIAL WAYS TO TACKLE THEM.

LACK OF TRUST AMONG THE GENERAL PUBLIC IN THE FINANCIAL SECTOR

This can be addressed with stronger data protection and privacy laws, better communication, education, and consumer awareness, as well as a well-developed and implemented consent framework.

LOW LEVELS OF FINANCIAL LITERACY AMONG THE GENERAL PUBLIC

This requires more targeted interventions and greater collaboration among different stakeholders in executing a strategy.

RAPID, SOMETIMES UNCONTROLLED, GROWTH OF PRODUCT INNOVATIONS

This requires an institutionalized platform for collaboration between private players and regulators. Sandboxes and test and learn approaches would help regulators and authorities gain better oversight.

UNDERDEVELOPED CONSUMER PROTECTION MEASURES AND POLICIES

This requires practical safeguards within the system to ensure protection for users.

EXECUTIVE SUMMARY

While there has been a significant advancement in access to financial services in recent years in the EECA region, there remain at least 121 million people[1] who are not a part of the formal financial sector. AFI member countries in the ECAPI have taken significant measures to expand financial inclusion in the region.

This includes building the necessary ecosystem for e-ID and e-KYC to enable hassle-free and streamlined access to financial products and services. As many countries in the region are in the process of building the supporting policies and infrastructure for e-ID and e-KYC, it would be important to consider technical and operational guidance on building robust e-ID and e-KYC systems. The AFI Eastern Europe and Central Asia Policy Initiative (ECAPI) has devised a framework that includes best practices and international experiences to guide the development of e-ID and e-KYC in the region. This framework takes into account how e-ID, and leveraging it for e-KYC, has successfully addressed the challenges of accelerating financial inclusion. The framework captures the best practices of some countries that can be implemented across others. Building a robust ecosystem for e-ID facilitates various use cases that in turn promote financial inclusion. Service providers and governments can leverage the e-ID platform to include, engage, and support population groups that might have previously been excluded or underserved.

The overall framework consists of the following three broad components:

- Policy development
- Infrastructure development and policy implementation
- Ecosystem development

These components detail specific principles that AFI members in ECAPI can consider while formulating policies related to digital identity and e-KYC. The principles have been formed for the growth of innovation in e-KYC and e-ID while adhering to Financial Action Task Force (FATF) recommendations. The principles presented in this paper address the major issues related to scaling the implementation of e-ID and e-KYC. Countries in the region can refer to the relevant principles depending on their current status and implementation of an e-ID and e-KYC platform. Considerations for the vulnerable and underserved have been made as a cross-cutting consideration with principles that are applicable across the framework.

The principles will need to be referred to by different authorities, relevant government ministries, and regulators who have the prime responsibility to implement various aspects of digital identity and e-KYC. The validity and importance of the principles will differ from country to country. The overall guidance on the principles presented in this paper can be adjusted to each country's requirements.

Building the right kind of policies, legislation, and regulations around e-ID and e-KYC are critical to advance financial inclusion. AFI member countries in ECAPI can consider enacting specific laws and guidelines governing the following aspects:

- KYC (AML-CFT), including e-KYC
- Identity and digital identity
- Data protection and privacy

In addition, countries are encouraged to develop a focused strategy or a guiding policy to drive financial inclusion. Clearly defined goals and objectives will help the stakeholders to take focused interventions to realize the vision. By designing and implementing more effective use cases to leverage the digital identity, this will also foster cooperation and coordination among the various stakeholders.

1 Demirgüç-Kunt, Asli, Leora Klapper, Dorothe Singer, Saniya Ansar, and Jake Hess. 2018. The Global Findex Database 2017: Measuring Financial Inclusion and the Fintech Revolution. Washington, DC: World Bank. Available at: https://globalfindex.worldbank.org

REGIONAL GUIDANCE - AN OVERVIEW OF THE PRINCIPLES

1

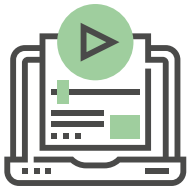
POLICY DEVELOPMENT

- **Principle 1:** Policy on digital identity
- **Principle 2:** Policy on KYC
- **Principle 3:** Policy on data protection and privacy
- **Principle 4:** Policy on establishing institutional and governance structures and ensuring cooperation

2

INFASTRUCTURE DEVELOPMENT AND POLICY IMPLEMENTATION

- **Principle 5:** Building technology and identification systems
- **Principle 6:** Building last mile connectivity
- **Principle 7:** Adopting user centric approaches and guidelines
- **Principle 8:** Developing exception handling protocols



3

ECOSYSTEM DEVELOPMENT

- **Principle 9:** Leveraging e-KYC for digital identity
- **Principle 10:** Leveraging interoperability
- **Principle 11:** Leveraging digital identity and e-KYC for financial inclusion
- **Principle 12:** Driving innovation

1

POLICY DEVELOPMENT

The guiding principles in this section will help build a cohesive and inclusive policy framework in the country.

This will allow for an enabling policy environment that supports the implementation of the best practices for e-KYC and leveraging it to increase financial inclusion.

GUIDING PRINCIPLE 1: POLICY ON DIGITAL IDENTITY

Regulators should build a comprehensive legal framework governing the use, scope, and management of digital ID. The legal framework should consider the country's context, supporting infrastructure, and priorities.

KEY ASPECTS

- Comprehensive legislation encompassing guidelines and policies on the use and applications of digital identity can be drafted. Key aspects that should be part of the regulatory framework of a country can include:
  - a. Objective and scope of use of the digital ID
  - b. Restrictions on sharing information, e.g. access and permissions for third parties
  - c. Data integration and interoperability
  - d. Details on data storage and management
  - e. Security and confidentiality of information
  - f. Roles, responsibilities, and accountability of the entity in charge
  - g. Grievance mechanisms and escalation
  - h. Special measures for women and vulnerable groups, amendments to existing laws to integrate forcibly displaced persons (FDP).
- To ensure the policies on digital identity are based on the relevant best practices and international standards, countries can take guidance from the FATF

EXPLANATION AND IMPACT

A clear and well-articulated policy or guideline helps stakeholders to make informed decisions on the use and management of ID and its various applications and increases compliance. This also helps the public and the private sector to expand the use cases and scope of digital identity while reducing the risk of fraud and data theft. An overall guiding legal framework on digital identity can therefore be formulated before the implementation of the digital ID program. It should also provide clarity to different stakeholders involved in the implementation of the ID system. The role of the public and private sector in supporting digital identity implementation and building the ecosystem for it should be addressed in the policy.

Most AFI member countries in ECAPI that have implemented digital identity have separate policies and guidelines on the identity system. For example, Armenia has a separate law[2] on digital identity systems

while countries such as Belarus and Uzbekistan are in the process of building a specific legal framework for the identity ecosystem before rolling out their digital systems.

Even where there is no national ID, biometric-based identity may serve as a de facto national ID because of its high degree of acceptance across financial institutions and businesses. For example, Belarus developed an Interbank Identification System (IIS) in 2016 through which all financial institutions and government bodies provide remote authentication services even where no national identification system has been implemented. The Unified Biometric System (UBS) in Russia allows people to access financial products and services through remote identification and e-KYC services. The UBS is due to receive "state information system" status so it can also be used for non-financial services.

Principle 1.1 Design elements of the digital identity system

The guidelines or policy on digital identity should clearly define the design elements of the identity system. The method for onboarding to the digital identity system can be determined based on the design elements of the system.

KEY ASPECTS

- The policy can specify the type of ID (foundational[3] or functional[4]) which is being implemented in the country. The decision needs to be taken considering the needs and objectives of the identity program.
- The quality of digital databases and the country context need to be assessed before deciding the mode of onboarding. Countries with advanced and trusted databases can choose automatic or push-based onboarding that will use the information available in the database to automatically sign users up to the digital identity system. Other countries can build the identity system from scratch by implementing a pull-based onboarding system that requires eligible users to sign up or register themselves.
- The authorities can issue guidelines on the requirements, eligibility, and process for onboarding people to the digital identity system. The registration process should be decentralized to enable people to register from remote places and via different channels. The guidelines should be inclusive and not impede any population group from being onboarded to the system.
- The registration system can be made flexible to allow people to be recognized by the gender they identify with as opposed to the gender assigned to them (at birth).
- To ensure maximum inclusion, the guidelines can promote zero or minimal costs for people to be onboarded to the digital identity platform.
- Authorities can arrange for special facilities in remote areas to include underserved and vulnerable groups in the digital identity system.
- Authorities can consider targeted initiatives to raise awareness among vulnerable and underserved groups on the importance of signing up or registering themselves for the formal financial system.

EXPLANATION AND IMPACT

Robust digital identity systems with widespread coverage provide a multitude of benefits to both the public and private sector. Full national coverage within the civil registration system provides a strong foundation for an identity management system. Entry into identity systems is provided through birth registration. Countries with poor and non-digitized civil registration systems should not mandate birth registration for enrollment in the foundational ID systems because these requirements will create additional barriers and unnecessary costs for people to access identity and will lead to exclusion. Countries with compulsory identity registration can consider providing identity credentials free of cost or at subsidized costs for those who cannot afford registration.

Most AFI member countries in ECAPI have robust civil registration systems and are building their ID systems digitally. Armenia presents a good example of building a strong ID ecosystem by digitizing its two important databases: civil register and population register.

2 Law of the Republic of Armenia. 2011. About ID cards (translated by AI). Available at: https://cis-legislation.com/document.fwx?rgn=98969

3 Foundational IDs are multipurpose IDs, such as a national ID and a civil registry, that provide identification for the general population. See, World Bank. 2019. ID4D Practitioner' Guide: Version 1.0 (October 2019). Washington, DC: World Bank. Available at: https://documents1.worldbank.org/curated/en/248371559325561562/pdf/ID4D-Practitioner-s-Guide.pdf

4 Functional IDs manage identification, authentication, and authorization for specific sectors or use-cases, such as voting, taxation, and social protection. Ibid.

Principle 1.2 Identity proofing

Regulators can enable different levels of identity proofing for convenient enrollment of the vulnerable groups to the ID system.

KEY ASPECTS

- Data can be verified with independent and reliable data or documents, such as birth certificates and civil databases, to the extent possible
- Exception methods, such as community proofing, can be allowed for users who do not have any document to prove their identity

EXPLANATION AND IMPACT

Complex registration and proofing requirements may further pose financial and logistical barriers for vulnerable categories of the population who may not always have access to supporting documents. To enhance the inclusion of vulnerable groups, authorities can allow alternative measures, including affidavits from the local government, frontline workers, teachers, and written statements by community members for identity proofing.

UNHCR's Biometric Identity Management System[5] for refugees can be used to register, verify, and target assistance for refugees and forcibly displaced persons. AFI member countries in ECAPI can consider easing norms to provide identity and verification services to refugees who face challenges such as the lack of recognition of their IDs and delays in getting IDs from current onboarding systems.

India's Aadhaar system adopted a risk-based registration method by allowing people without any supporting document to use approved introducers to ascertain their identity. Gazetted officers could issue signed letters with applicant's photo and details to attest the identity of those without supporting documents.

Principle 1.3 User credentials

Authorities can consider user preferences and features such as accuracy, safety, and functionality before identifying the most suited credentials for digital ID.

KEY ASPECTS

- Authorities can evaluate the most appropriate credentials for the general population of the country. Credentials can be evaluated based on the required functionalities and levels of security.
- Authorities can promote multi-stakeholder consultations on the design, accuracy, use cases, costs, and limitations of the credentials.
- Authorities can ensure the chosen credentials are inclusive and do not cause barriers to use for any segment of the population. For example, physical credentials will help people authenticate safely in areas with low connectivity while digital credentials will be more suited for areas with high internet connectivity.
- Authorities can consider issuing multiple credentials to give more choice and convenience to people.

EXPLANATION AND IMPACT

Issuing multiple credentials will promote equal use of the digital ID and the associated services among different user segments. It will also ensure that no additional barriers to use are created for any segment of users.

For instance, Estonia offers both physical ID and digital ID to users. Since it has a high penetration of mobile phones and a strong network infrastructure, it offers different kinds of mobile ID for digital authentication, e-signatures, and access to online services. Also, Nigeria's mobile ID, Singapore's SingPass Mobile, and India's mAadhaar are a few more examples of mobile versions of e-ID. Most AFI member countries in ECAPI have high mobile penetration rates and strong network connectivity. This presents an opportunity for governments to expand ID coverage by providing mobile identity and mobile-based PINs. For example, In 2018, Armenia tested the Mobile ID (mID) system for personal identification and e-signature.

GUIDING PRINCIPLE 2: POLICY ON KYC

Regulators need to formulate dedicated laws and guidelines on the various aspects of AML-CFT, including KYC and e-KYC.

KEY ASPECTS:

- Regulators need to promote and ensure adherence to global standards such as FATF while formulating policies on KYC, AML-CFT, and e-KYC.
- A strong AML-CFT guideline should be made after identifying the risks and challenges faced by financial institutions, regulatory requirements, and

5 Biometric Identity Management System, Enhancing Registration and Data Management, The UN Refugee Agency. Available at: https://www.unhcr.org/550c304c9.pdf

the potential impact of non-compliance with global standards.

- Regulators need to clearly define policies on KYC, including guidelines on a tiered or risk-based approach to KYC, accepted documentation to conduct KYC, and compliance with AML-CFT guidelines.
- A risk-based approach needs to be applied to digital identification or verification so that the greater risks are prioritized and receive greater attention. Risk assessments can be done on multiple levels:
  - customer/ country/ geography
  - products / services/ transactions/ channels
- Regulators can mandate regular assessments of KYC policies to understand if there are any limitations that affect vulnerable populations and the challenges faced by stakeholders in complying with AML-CFT recommendations. They can then revise the KYC policies, as appropriate, for the jurisdictional context and identity ecosystem of the country.
- Authorities need to build economic cost structures for KYC services and ensure the cost of compliance for stakeholders is viable.
- A dedicated policy and framework can be devised to promote and regulate e-KYC transactions in the country. The policy should come with clear guidelines on:
- The scope of simplified and regular e-KYC for different stakeholders based on the risks identified
- Applicability of e-KYC (for people with digital ID and exception measures for those without digital ID)
- Technology guidelines and specifications for e-KYC
- Collecting user consent for data processing, storage, and management
- Authorization of third-party access to data
- Risk assessment and monitoring
- Penalties for data breach by a stakeholder
- Cost structure for public and private players

EXPLANATION AND IMPACT

Policies on AML=CFT and KYC are designed to protect against financial fraud and reduce terrorism financing. However, raising compliance requirements has increased costs and complexity for banks and other financial institutions, and has increased challenges in cross-border payments and correspondent banking relationships. Building robust policy on the implementation of KYC and AML-CFT recommendations is crucial to help stakeholders keep pace with evolving rules and regulations and to effectively manage AML-CFT risks. It is also imperative to adopt a risk management approach to ensure that the steps taken to prevent or mitigate against money laundering and terrorism financing correspond well with the risks identified.

Most AFI member countries in ECAPI do not have specific guidelines on e-KYC and regulate it under the general principles of KYC. Financial institutions choose the tools and techniques for e-KYC, considering the possible risks. Banks and other financial institutions are recommended to carry out risk assessment exercises and seek references for high-risk individuals. Most countries, however, follow a risk-based approach for KYC and allow lower levels of identification and monitoring for low-risk individuals. For example, Russia allows people without proof of identity to conduct transactions below a specified threshold.

National banks and financial intelligence units (FIU) of the AFI member countries in ECAPI regulate and supervise AML-CFT compliance. They conduct audits and inspections of supervised entities that are subject to financial monitoring by AML-CFT legislation and apply sanctions for any breaches.

GUIDING PRINCIPLE 3: POLICY ON DATA PROTECTION AND PRIVACY

Regulators need to formulate a national law or policy on data protection and privacy for individuals. The law needs to clearly define data protection safeguards, including rules on the collection, use, and management of data.

KEY ASPECTS

- Countries can seek guidance from GDPR principles on privacy by design before formulating data protection and privacy laws, if applicable. The policy needs to assure users that their privacy is being respected on every platform where their data is being used, processed, or stored.
- The laws need to clearly state what data can be collected, including biometric information, personally identifiable information (PII), and demographic data. The key elements of the law should cover:
  - Collection of minimum data

- Mandatory consent from the data fiduciary for the processing of personal data
- Details of scenarios of when consent would not be required e.g. a court order
- Special provisions for children (collecting limited demographic information and linking to the legal guardian) and vulnerable groups such as refugees
- Access to third parties
- Data localization and policy on cross-border data transfer
- Privacy by design principles extended to data fiduciaries
- Classification of sensitive data; these could be fields of data which, if disclosed, might cause harm to the data subject. Such data, if collected, should be classified into tiers to ensure additional privacy and security by limiting third-party entities from fully accessing data
- Penalties for mishandling of data
- Deletion of personal data when their original purpose of collection has expired

> The law can also provide guidelines on how to conduct regular privacy audits and assessments. This will ensure that data protection and privacy measures are implemented according to law and any deviations are highlighted and corrected.

> Regulators can ensure the use of the principle of proportionality by collecting minimum data from citizens. There should be guidelines and mechanisms that allow amendments and deletions of inaccurate data. Authorities, including financial institutions, should respect user privacy and adhere to the principles of proportionality by not collecting more data than is necessary.

EXPLANATION AND IMPACT

Clear and articulate data protection measures guarantee appropriate levels of security against any form of data theft or fraud for both users and stakeholders. It helps stakeholders understand the level of data protection measures to be taken to comply with the established guidelines. A robust and well-established regulatory framework on data protection and privacy will foster a high level of trust in the overall system among users and stakeholders.

Most AFI member countries in ECAPI govern data protection by using legal instruments on personal data and constitutional rights. However, these need to be amended to bring them into line with the international trends and principles on data protection and privacy.

GUIDING PRINCIPLE 4: ESTABLISHING INSTITUTIONAL AND GOVERNANCE STRUCTURES AND ENSURING COOPERATION

Regulators need to build independent, transparent, and accountable institutional structures governing AML-CFT, digital identity, e-KYC, data protection, and financial inclusion in their respective countries.

KEY ASPECTS

> The institutional arrangements for the identity authority can either be a system administrator or an agency within the existing ministry or a statutory authority governed by a separate board, with stakeholders from the relevant government departments

> Regulatory coordination among different entities managing digital ID and e-KYC systems should be promoted

> Regulators need to ensure the institutional structures are given clear responsibilities to meet their stated goals and objectives independently

> The institutions need to conduct regular audits and should be answerable for issues related to the digital identity program

> The institutional structure needs to be financially autonomous, with independent budgets, to avoid conflicts of interest

> Regulators can mandate regular monitoring and capacity-building of the institutional and governance bodies to ensure course corrections, if required

EXPLANATION AND IMPACT

Safeguarding personal data and implementing digital identity systems and e-KYC require collaboration among multiple stakeholders. It is therefore important to establish independent institutional structures to govern and drive the different systems.

AFI member countries in ECAPI should push for increased coordination among different bodies governing the systems crucial to e-KYC and digital identity.

Armenia's ID system presents a good practice as it is built on cooperation among institutions responsible for the management of civil registration and the identity system. Both the systems are managed by separate agencies and are responsible for different aspects of digital identity management.

2

INFRASTRUCTURE DEVELOPMENT AND POLICY IMPLEMENTATION

The guiding principles in this section have been drafted to support the implementation of the overall system.

They provide the technical features and capabilities that can be considered to ensure a robust system that meets a country's current needs as well as evolves to allow for innovation and sustainability of the system.

This section also focuses on features that will maintain security and privacy, and approaches that make the e-ID and e-KYC systems more user-centric.

GUIDING PRINCIPLE 5: BUILDING TECHNOLOGY FOR IDENTIFICATION SYSTEMS

Regulators can ensure that the technology used to develop the identity system is robust, has relevant capabilities, and is customizable.

KEY ASPECTS

- Regulators need to promote the building of trust frameworks for digital identity systems comprising technical specifications, laws, and policies related to data protection. A consent framework should also ideally be worked into the design of the system to ensure a user-centric approach is followed.
- Authorities need to ensure that key features such as deduplication and fraud detection processes, and privacy by design, are embedded in the technology infrastructure.
- Authorities need to oversee and ensure that the technology and devices used will support multi-modal authentication (more than one biometric), offline authentication and onboarding, and other such exception handling procedures.

COMMON BIOMETRIC AUTHENTICATION MODES


Iris scan


Facial scan


Fingerprint scan


Voice recognition

- The architecture can also include the development of application programming interfaces (APIs) that can be leveraged for different use cases, such as e-KYC by third parties. APIs should be made easily available to streamline access to data for productive use.
- Technical standards for the system need to adhere to international norms to ensure best practices are followed. Standards on biometrics, smart cards, digital signatures from standard-setting bodies such as ISO and NIST are integral to developing a system that is relevant and interoperable across regions.

- Consider open-source technologies to avoid vendor lock-in and ensure minimum cost implications.

EXPLANATION AND IMPACT

A robust technology architecture will ensure sustainable development and upgrades to the system in line with international best practices. Adherence to international standards will ensure the implementation of universally understood protocols necessary for operation, performance, compatibility, and interoperability.

For instance, financial institutions in Russia can access its Unified System of Identification and Authentication (USIA) using APIs or a government electronic communication system. Similarly, in Armenia, access to the national identity database is possible only through the government's interoperability platform via APIs.

GUIDING PRINCIPLE 6: BUILDING LAST-MILE INFRASTRUCTURE

Regulators need to ensure the building of strong and standardized last-mile infrastructure for identity systems to improve their connectivity and reach.

KEY ASPECTS

- Authorities need to ensure robust security measures for the systems that store identity data, enable networks to access the systems, and any other backup systems.
- Authorities can standardize the type of devices used for last-mile authentication to ensure strict adherence to safety, quality, and technical standards.
- Authorities need to encourage the use of multiple channels to reach end-users, the leveraging of different networks, and ensure that services are accessible and cost-effective.
- Digital financial services can be obtained via a variety of digital channels, including mobile phones, personal computers, POS terminals, and ATMs, among others.
- Design inclusive digital infrastructure to provide easy reach and access for vulnerable groups specifically and ensure assisted models of access are available.
- Agency models can be seen as an important tool for increasing financial inclusion outside of affiliate networks of financial services providers. Such digital channels make it possible to expand the provision of financial products and services to many individuals, including in regions not covered by financial services. For most consumers, banks are the only available provider of formal financial services. There is limited product diversification and the non-bank financial institutions are still small and have low penetration.
- Last-mile connectivity needs to have device-agnostic reach and have options for offline services.

EXPLANATION AND IMPACT

The success of this system and the use cases that are built around it will ultimately depend on the impact and outcome at the last-mile level. The benefits to society and the system's users or beneficiaries are crucial to the success of the overall system. A digital ID can bring several benefits to previously unbanked and underbanked groups; however, efficient networks and last-mile connectivity are imperative to realize these impacts.

GUIDING PRINCIPLE 7: ADOPTING USER-CENTRIC APPROACHES

Regulators need to ensure that the guiding policies on digital identity and its use cases (including e-KYC) adopt user-centric approaches and allow users complete control of their data.

KEY ASPECTS

- The policies on identity and its use cases (e-KYC) need to extend more control to users by allowing them to:
  - Provide consent and authorization to third parties and revoke consent
  - Rectify, update, and erase information
  - Lock biometrics
  - Track transactions where personal data was accessed or processed
  - Receive just in time notifications and alerts
  - Seek redress in case of identity theft or data breach
  - Port information
- Authorities need to ensure users are provided with adequate information on the purpose of data collection so that users can give informed consent
- Regulators need to promote the building of a consent management architecture to support the overall consent collection, storage, and management of user data
- Authorities can consider providing easy accessibility to user services and multiple channels for consent management

- Authorities can take special measures to educate underserved and vulnerable users on informed consent and ensure that individuals provide the required information with complete knowledge of the associated risks

EXPLANATION AND IMPACT

The implementation of digital identity leads to the proliferation of systems that capture, process, and analyze a range of personal data. Access to various services and products requires users to share sensitive aspects of their lives with service providers. Although most systems require users to give their consent before allowing anyone to process their data, this consent is often considered mandatory by users. Concerns about the privacy of personal data are increasing as cases of data privacy breaches, cyber threats, and data leaks of sensitive information are on the rise. A proper consent management framework and user-centric policies will make users more informed and empowered to control and guard their data. It is equally important to communicate the consent management framework and other available user services in the right way and ensure comprehension. Specific measures to increase user literacy and user control of consent related to identification systems will also foster a culture of understanding and trust.

Armenia has built a robust e-citizen platform that helps its citizens to exercise their right to know how their personal data is processed as well as to seek redress if they believe their personal data was processed in violation of the law. The platform enables individuals to view their data kept in state databases and to monitor the log of requests for their data by third parties. Citizens can seek immediate redress if they have not consented to share their data with the data processor.

Kazakhstan[6] allows users to know the purpose of processing their data, to block or delete collected data, withdraw consent, and seek compensation in case of privacy violation.

Users in Belarus and Russia[7] are allowed to withdraw their consent, access personal data, request modification and deletion of their data, which is excessive, or processed unlawfully.

GUIDING PRINCIPLE 8: DEVELOPING EXCEPTION HANDLING PROTOCOLS

Regulators need to conduct an assessment of all possible challenges and risks associated with the implementation of the digital ID system and define its exception handling protocols.

KEY ASPECTS

- Authorities can conduct a thorough assessment of risks and challenges in the system. These should be documented and mitigation strategies should be included. The entire lifecycle of the system should be considered and challenged from the perspective of design, onboarding to KYC, and authentication processes should be detailed.
- Specific provisions to cover different categories of the population can be developed, including for the vulnerable. Offline solutions and exception management should be devised to improve last-mile access. It is challenging to collect biometrics from vulnerable populations or those in remote areas with limited connectivity and literacy. Even infants, the differently-abled, the elderly, and some manual workers with worn-off fingerprints due to their work, might find it challenging to record biometrics.

EXPLANATION AND IMPACT

With a system that needs to meet the needs of an entire country's population, there will be some exceptions to the norm that require additional processes to ensure there are no disturbances or exclusions in delivering its services. For a universally accepted system that benefits all citizens and users, it is imperative to build the technology and ecosystem for it that ensures all exceptional cases can be addressed and accounted for.

6 Alexeyev, Anton, Oleksandr Melnyk, Oksana Voynarovska, and Maria Otashenko. 2020. “Data protection compliance: an essential guide from Kazakhstan, Russian and Ukraine”. Ius Laboris Insights (blog). December 7. .https://iuslaboris.com/insights/data-protection-compliance-an-essential-guide-from-kazakhstan-russia-and-ukraine/

7 Ibid.

3

ECOSYSTEM DEVELOPMENT

The guiding principles in this section will help develop the ecosystem around e-ID, including e-KYC capabilities.

Developing different use cases and interacting with various stakeholders will be imperative for the system's sustainability and to leverage it to benefit public and private sector players.

This section also provides inputs and best practices to drive financial inclusion and encourage innovation.

GUIDING PRINCIPLE 9: LEVERAGING DIGITAL ID FOR E-KYC

Regulators need to clearly define the scope of use of the digital ID and regulations should explicitly allow its use for e-KYC in the country, with guidelines.

KEY ASPECTS

- Authorities need to ensure the identity system allows for tiered KYC following the policy of the country.
- Authorities and stakeholders can collaborate on and publish a standardized list of different levels of services using the digital ID, such as authentication and e-KYC (demographic and biometric) and auto-fill user data, depending on the needs of the country and main requirements of industry players.
- In the absence of adequate documents, alternative forms of identification need to be made acceptable as per global AML-CFT standards, for example, a letter from a village head, validation through a public officer, etc.
- Authorities need to define the rules of engagement for third-party stakeholders who want access to the system. This should include the minimum requirements and permissions required for access, the steps and procedures for gaining access, and what is required of the third party in terms of data protection and security measures.
- Authorities and system developers can ensure there are easy channels of access to the system, such as APIs and web access, with high security and privacy safeguards. Channels should also be cost-effective and streamlined to ensure minimum disruption.
- Authorities can consult with industry players to understand their willingness to pay for e-KYC and authentication services and use this to build a costing model. This will ensure some sustainability for the system and revenue for the system administrators to fund upkeep and upgrades. Costing should be economical, and in line with industry expectations.
- Authorities can also build a monitoring system for all stakeholders who have access to the system.

EXPLANATION AND IMPACT

An e-KYC ecosystem developed on top of the digital ID provides some revenue to maintain and update the overall system. Uniform access for industry players to leverage the system will promote fair market access

and also allow them to prepare their internal systems. Developing this ecosystem will ensure the longevity and productive use of the digital ID platform and savings of costs and time for various stakeholders. Building a solid case of e-KYC in one sector will also encourage other stakeholders to consider and build more use cases for the system.

Several AFI member countries in ECAPI have implemented e-KYC for financial services using their national identity systems (e.g. Mongolia) or with the identity systems developed by their central banks (e.g. Belarus, Russia). These countries have significantly improved their e-KYC systems over the years. However, financial services providers in the region find it costly to implement effective and secure e-KYC measures. Authorities should stress on creating public-private partnerships to create revenue flows and ensure sustainability. This will reduce the financial burden of establishing and running a digital ID and e-KYC system. However, authorities should take care to not transfer the high registration costs to the public and service providers as this can limit the system's usage.

GUIDING PRINCIPLE 10: ENABLING INTEROPERABILITY

Authorities need to ensure that digital identity systems are interoperable with domestic systems to effectively communicate with other systems, such as civil registration systems and population registers.

KEY ASPECTS

- Authorities can engage with multiple stakeholders to promote discussion and provide guidance on interoperability and use cases that can leverage the digital identity infrastructure.
- Authorities need to address regulatory requirements to facilitate interoperability for:
  - Delivery of government services
  - Social protection delivery of different departments and ministries
  - Formal financial institutions
  - FinTechs
  - Non-financial institutions, such as telcos
  - Third-party authorized e-KYC/KYC companies

EXPLANATION AND IMPACT

A high level of interoperability ensures that different ID systems are recognized by other systems in operationally effective ways. A high level of interoperability reduces operating costs and fosters administrative savings for government departments. It also helps in removing duplicate data or obsolete databases and ensures sustainable use of the data by keeping them relevant. Interoperable ID systems enable public and private players to effectively authenticate and verify individuals. Despite the plethora of benefits, interoperability can also pose a risk for privacy and data security. Identity systems should therefore limit data sharing to the minimum necessary. Authorities should ensure that no personal data is at risk of fraud or theft due to interoperability.

The ID systems must be interoperable with civil registers. Timely updates to the ID systems through birth registration and deletion of records through death registration are critical to ensure the integrity of data. Creating an e-ID using birth registration can ensure the inclusion of all people in the ID system. AFI member countries in ECAPI have built-in strong domestic information exchange systems to allow interoperability with government databases. Armenia offers an important example by allowing data interoperability among various government departments and databases. The two building blocks of identity management, which are the civil register and the population register, are digitized, well-integrated, and interoperable. The population register automatically transfers identity information to the civil register each time a vital life event (birth, death, marriage, divorce, etc.) is recorded in the civil register.

Similarly, the e-Mongolia platform, now being linked with the national databases (Khur and Dan) will provide citizens with reliable and online state services.

GUIDING PRINCIPLE 11: LEVERAGING DIGITAL ID AND E-KYC FOR FINANCIAL INCLUSION

Regulators need to ensure that the digital identity systems and e-KYC are utilized to their full potential to drive financial inclusion.

KEY ASPECTS

- Develop and update the national financial inclusion strategy (NFIS) to ensure a holistic approach is taken, involving all relevant stakeholders. The NFIS should contain strategies to improve access to financial services in remote areas and leverage technology to enhance the quality of products and services. The NFIS should detail steps to be taken

while considering the local environment and challenges, and assign clear responsibilities and targets. The NFIS should also include a timeline, milestones, and targets. The targets should be set using an outcome-based approach to ensure measurable and clear impact.

- Launch specific policies and regulations that have a clear chance of accelerating financial inclusion in the country. These regulations and policies can allow for specific products or services in the market by relaxing some of the KYC norms or by making products more affordable and leveraging digital IDs. Designing products for first-time users will need to consider affordability, financial literacy, last-mile connectivity, use cases, and ensure that these meet their needs and requirements. By receiving their pensions in commission-free accounts, such as in Armenia, pensioners can use the money digitally for other use cases.
- Financial services providers should develop products tailored to the needs of women and other vulnerable populations and take into consideration the agency of women. A study to identify their main barriers should be conducted by authorities to inform and provide guidance to service providers who are designing products. Issues such as access to a mobile phone, how comfortable they are in dealing with last-mile infrastructure, agency, and behavioral biases that affect the way women interact with financial services providers, should inform product development and marketing.
- Develop more relevant use cases and leverage e-ID for subsidy transfers. This will allow a convenient, safe and fast mechanism to exchange data required for transfers and interactions between citizens and the state.
- Encourage other stakeholders in the ecosystem to share the responsibility for accelerating financial inclusion by providing incentives to ensure their participation. Consider options such as tie-ups with government ministries for social security payments, allow banks to act as sponsor banks for selected programs, and receive incentives for bank accounts opened and transfers made. Assess the feasibility of subsidizing infrastructure costs of telcos that are willing to build network infrastructure and strengthen connectivity in remote areas.
- Ensure that digital financial literacy is core to the work of the NFIS. Ensure targeted communication of users by employing various approaches that consider behavioral aspects and incorporate the same in the program design. Concepts such as orality[8] mental models, etc are important to be considered to create curriculum and approaches that are suited to different groups and their needs.

EXPLANATION AND IMPACT

First-time users of financial services have different needs and biases to be met and addressed to drive up usage. It is imperative for success to design and develop not only products, but marketing and customer service procedures, to ensure their needs are met. In countries where the identity system is pull-based, this population is also traditionally excluded from having any identity documents. Accelerating financial inclusion to achieve complete coverage of the entire population will require the support and buy-in of several stakeholders in the financial sector and other complementary sectors. Incentivizing stakeholders is key to get active participation as well as hold them accountable for meeting targets. Since these stakeholders are working on the ground, they also have better reach and can mobilize populations more effectively.

There is a great variation in the financial inclusion status of AFI member countries in ECAPI. Countries such as Armenia and Tajikistan have seen the greatest increases in bank account penetration. This underlines the important role of digital payments. The number of bank accounts in Tajikistan[9] increased from 3 percent in 2011 to 46 percent in 2017 mostly due to the government's efforts to transfer pensions and other payments to individuals through the banking system. However, there is still considerable scope to increase account ownership in ECAPI member countries by transferring social security payments directly into the bank accounts of recipients.

Despite a high penetration of bank accounts in Mongolia, it faces multiple challenges such as a low savings rate, costly financial resources, and poor financial literacy among individuals. According to the Financial Regulatory Commission, financial literacy is inadequate and a considerable gap exists in knowledge between urban and rural, and rich and poor communities. Financial literacy is weak specifically among women.

8 Orality is a form of thought and verbal expression where literacy is unfamiliar to most of the population. It stresses on the use of speech rather than written communication.

9 Demirgüç-Kunt, Asli, Leora Klapper, Dorothe Singer, Saniya Ansar, and Jake Hess. 2018. The Global Findex Database 2017: Measuring Financial Inclusion and the Fintech Revolution. Washington, DC: World Bank. Available at: https://globalfindex.worldbank.org

GUIDING PRINCIPLE 12: DRIVING INNOVATION

Regulators can ensure to test new opportunities and approaches to drive innovation that leverages the digital identity system

KEY ASPECTS

- Authorities can consider setting up a regulatory sandbox in the country or a regional regulatory sandbox[10] to allow for innovation and foster innovative thinking.
- A more economic model of a test and learn initiative can also be taken in countries where there are some constraints.
- The sandbox can allow private players to take advantage of relaxed regulations to drive innovation and regulators can ensure oversight as well as proactively plan for any regulatory changes that may be required. This also ensures a synergistic approach to developing efficient products and services.
- Authorities need to identify key sectors or priority areas to promote innovation and encourage private player participation, including:
  - Cost-effective ways to deliver services through technology-enabled channels including e-KYC
  - Remote onboarding tech by leveraging digital ID for different services and products
  - Low-cost credit and alternative credit rating options for people with no formal credit/score

EXPLANATION AND IMPACT

A sandbox setup creates a cohesive and beneficial space for all key stakeholders. Regulators can monitor private players looking to innovate as they have the visibility to ensure that deviations in policy are within suitable boundaries that they can determine. It also allows private sector companies to experiment and develop innovative solutions without sanctions or push back from regulators.

Most AFI member countries in ECAPI have introduced regulatory sandboxes to drive learning and innovation in financial services. The Bank of Russia introduced its regulatory sandbox in April 2018. This enabled the testing and development of new financial services and technologies which, in turn, required amendments to existing regulations.

Kazakhstan is developing a policy on building a digital economy. It has launched regulatory sandboxes and the Digital Kazakhstan[11] program for the development of FinTech in the country.

The Financial Regulatory Commission of Mongolia has developed a draft regulation, Regulatory Sandbox, to establish a legislative framework in the country to support, design, and test new technology-based products and services.

10 AFI PIRI. 2020. Pacific Regional Sandbox Regulatory Guidelines. Regulatory Guideline No. 01. March 2020. Pacific Islands Regional Initiative under Alliance for Financial Inclusion. Available at: https://www.afi-global.org/sites/default/files/publications/2020-03/PIRI_Regulatory_Guideline_digital.pdf

11 https://digitalkz.kz/en/

CONSIDERATIONS FOR VULNERABLE AND UNDERSERVED POPULATIONS

Across contexts, women face gender-based barriers that make it hard to obtain, use, control, and manage official IDs.

At the same time, other population groups such as the elderly, illiterate, and disabled are often underserved as they face challenges in obtaining, using, and managing their IDs. These barriers can be legal, economic, procedural, social, or a combination of them. This has resulted in a situation where women and the poorest are at a 40 percent[12] greater risk of being excluded from foundational ID systems.

The absence of an ID limits the financial, social, and political participation of women and other vulnerable population groups. Limited agency, mobility, literacy, and control of assets are the major barriers faced by vulnerable and underserved groups. It is therefore crucial to consider the following parameters to design policies, laws, and guidelines on digital identity, AML-CFT, data protection, and privacy and financial inclusion, that serve all population groups. Some considerations include:

1.ACCESSIBLE INTERFACES

The design and implementation of all beneficiary-facing interfaces across each stage of the ID lifecycle should be accessible and sensitive to the needs of women and other population groups with mobility issues. This includes increasing the level of comfort for women to transact at the interface, especially at the last mile. For example, this can be facilitated with women-only registration points, dedicated registration days for women, and by recruiting women agents to help manage the IDs or update them for any changes such as marriage or divorce, among others. Interfaces, especially in remote areas, should also be made oral-friendly. This will ensure the inclusion of population groups who are not comfortable and familiar with written communication and respond better to intuitive iconography and clear visual cues. This also applies to any beneficiary-facing applications and websites that are used for services and interaction.

2. SOCIAL CULTURAL NORMS

To advance the agency of women, the process of accessing IDs and their use cases should tackle social norms that deter women from using them. For instance, women in some cultural contexts may be discouraged from registering for an ID because they would have to interact with male officials or travel alone to obtain their ID documents. Similarly, people living in remote areas, the sick, and the elderly are less likely to travel to the registration points for onboarding to the identity system. To address their needs, administrators of ID systems can conduct social norm diagnostics for different contexts to understand the effect of social and cultural factors on women's agency as well as the overall access, use, control, and management of IDs for vulnerable groups.

3. TRANSPARENCY AND COMMUNICATION

Since women and vulnerable groups such as the illiterate and those living in remote areas are less aware of the benefits of obtaining identity documents and less confident to navigate through complex and opaque systems, authorities should ensure adequate communication and transparency for the use cases of the identity systems, and the opportunities for women and other vulnerable groups to avail themselves of them. Key developments in the application, use, and any changes to the scope of use cases need to be communicated clearly. An effective and inclusive ID should communicate effectively in language that women can relate to. The information to be communicated should be identified based on how to overcome the contextual social norms that hinder women's empowerment and agency and help inculcate the need for IDs among women.

Considering these additional principles to design or upgrade current systems will ensure that the challenges posed by limited agency, mobility, literacy levels, and ownership of assets are mitigated to some extent. These principles can be applied throughout the lifecycle of the ID system to ensure targeted interventions that benefit women. These would also go a long way in addressing similar challenges among other vulnerable and disadvantaged groups.

12 World Bank. 2019. Global ID Coverage, Barriers, and Use by the Numbers: An In-Depth Look at the 2017 ID4D-Findex Survey, Washington, DC: World Bank. p. 6. Available at: https://documents1.worldbank.org/curated/en/727021583506631652/pdf/Global-ID-Coverage-Barriers-and-Use-by-the-Numbers-An-In-Depth-Look-at-the-2017-ID4D-Findex-Survey.pdf

ANNEX 1: COUNTRY-WISE SITUATIONAL ANALYSIS

ARMENIA - STATUS

POLICY

Armenia[13] has specific laws and regulations on social services numbers (SSN), identity cards, and data protection. Every Armenian citizen has a unique and permanent SSN that also serves as their identification number for life. The SSN is automatically granted with a birth certificate or when obtaining Armenian citizenship. The identity card has an embedded chip with e-ID and signature certificates. Armenia has a strong e-citizen platform that helps individuals to control and manage their personal data and seek redress in case they are notified of a data breach. SSN has separate governance and institutional structures with an advanced level of interoperability among different systems.

INFRASTRUCTURE

In Armenia, citizens have both physical and digital IDs. MobileID has also been rolled out and the government is developing a system based on a mobile application that will not require additional hardware (as in the case of e-ID, where a special card reader is needed to be connected to the computer), or Usim cards (for enabling mobile ID) for using electronic identification and signatures. Citizens register within the application to gain access to different platforms and online services with their digital ID. Armenia adheres to FATF recommendations on AML-CFT and has introduced a risk-based approach to KYC. The country has not implemented e-KYC but is developing procedural norms for it.

ECOSYSTEM

Armenia has a strong network connectivity infrastructure but needs to take targeted measures to boost financial inclusion and digital payments, especially for women and other vulnerable groups. The low level of use of bank accounts and micro-savings are some of the financial inclusion challenges in Armenia. The Central Bank of Armenia is considering the development of regulatory sandbox.

BELARUS - STATUS

POLICY

Belarus has laws, regulations, and guidelines on identification, data protection, and KYC. It has issued biometric passports and national identity cards since September 2021. Belarus has adopted a draft data protection law that defines and sets up:

- categories of personal data
- the process for cross-border transfers,
- the creation of an authorized oversight body
- responsibilities for violation

Belarus has adopted a series of resolutions to bring its financial regulatory framework in compliance with the revised AML-CFT recommendations. Specifically, the government tightened internal control and made recommendations on risk management to the financial organizations in the country. However, financial institutions need to increase transparency and accountability to gain public trust.

INFRASTRUCTURE

The development of a national identification system (a unified system of identification and authentication of individuals and legal entities) is in progress and could start operating in 2021. ID cards will replace Belarusian passports. ID cards are intended to serve as personal identification documents inside the country. An ID card is a plastic card that contains a microchip. The microchip stores biometric identification records and a cryptographic authentication token. The KYC service is rolled out through the interbank identification system (IIS) which is an interesting example of the financial system's technological development. The system provides remote personal identification and allows different financial services to be received from financial institutions online. All supervised entities in Belarus understand and apply the enhanced customer due diligence measures (CDD) in the cases determined by the FATF. The legislation in Belarus does not advocate the application of simplified CDD measures.[14]

13 Dokovic, Zoran. 2019. Armenia, Case Study 1. In, Compendium of Good Practices in Linking Civil Registration and Vital Statistics (CRVS) and Identity Management Systems. Ottawa: Centre of Excellence for Civil Registration and Vital Statistics Systems. Available at: https://www.data4sdgs.org/sites/default/files/2019-12/CRVS_Armenia_e_WEB.pdf

14 EURASIAN GROUP on combating money laundering and financing of terrorism. 2019. Mutual Evaluation Report of the Republic of Belarus. Available at: https://www.fatf-gafi.org/media/fatf/documents/reports/mer-fsrb/EAG-Mutual-Evaluation-Report-Belarus-2019.pdf

ECOSYSTEM

Belarus has strong financial inclusion strategies and a high penetration of bank accounts. However, it needs to take focused measures to build financial literacy and expand financial services among the underserved and vulnerable.

KAZAKHSTAN - STATUS

POLICY

Kazakhstan has laws and guidelines on identification and data protection. The law on personal data in Kazakhstan has provisions to ensure consent from users. The Ministry of Digital Development, Innovations and Aerospace Industry will implement the principle of digital consent and revocation to allow individuals to control the use of their personal data

Regulatory agencies regularly inspect the reporting entities subject to the AML-CFT Law[15]. The reporting entities, however, lack resources and expertise to properly ensure compliance. Further, all reporting agencies, except banks, face challenges in implementing a risk-based approach to customer due diligence (CDD) and employ a blanket approach instead.

INFRASTRUCTURE

An identity card is issued to citizens from the age of 16. A passport is also considered an identity document. All citizens of Kazakhstan permanently residing in its territory must have an identity card. Kazakhstan has not yet established a unified identification system.

ECOSYSTEM

Kazakhstan does not have a national financial inclusion strategy in place.

MONGOLIA - STATUS

POLICY

Mongolia has specific laws on identity cards, data protection, and KYC. It has adopted a risk-based approach to KYC and has introduced e-KYC for a range of financial services providers following sector-specific laws and regulations. To comprehensively and effectively conduct e-KYC, all forms of information such as proof of identity and proof of address are requested from the customer. The documents submitted by customers can be verified by the government information exchange system (known as Khur and Dan) which effectively allows service providers to conduct e-KYC on a reliable government database. A common challenge for financial services providers is the lack of a publicly available list of politically exposed persons which makes identification of PEP's quite difficult. Additionally, publicly available information on beneficial ownership is inadequate, and the lack of such information creates complexity with the implementation of e-KYC.

Mongolia's Financial Stability Council has implemented the Financial Access Improvement Programme so that the legal environment facilitates the market entry of technologically advanced products and services. As the range of financial products and services expands, the cost of services will decrease. Together with improved financial education of citizens, this will create conducive market conditions for the provision of financial services cheaply, easily, and quickly. Mongolia has a high level of gender equality, and almost 96 percent of the population has at least one account in financial institutions. The laws, regulations, and current practices do not discriminate against gender, which leads to no gender inequality in access to financial services.

INFRASTRUCTURE

A compulsory smart ID with an embedded chip securing all personal data has replaced the identification card system. This information is available in the national database (Khur and Dan). while the credit information database is linked to various government entities, such as the Election Commission and the Tax Department. Thus the Khur and Dan systems are being made part of the e-Mongolia unified platform towards digitalizing the nation. Mongolia has built a strong identification infrastructure as its systems can promptly retrieve information from the state service (TUTS) with the use of fingerprints and electronic ID of the person. There is a need to adopt a national strategy on AML-CFT to fully implement the FATF Recommendations and strengthen AML-CFT capacity. Mongolia remains in enhanced follow-up on progress to strengthen its implementation of its AML-CFT measures, which allow enhanced CDD for high-risk areas.[16]

ECOSYSTEM

e-KYC is already implemented in the majority of financial institutions, where constant effort is made to improve the safety and security of e-KYC measures. Financial institutions, securities companies, insurance companies, etc, follow a risk-based approach to conduct e-KYC. Depending on the risks associated

15 Jersey Trust Company. 2018. Kazakhstan: Risk and Compliance Report. March 2018. Available at: http://www.knowyourcountry.info/files/Kazakhstanaug14_6.pdf

with the customer, further information is requested, and enhanced CDD is then conducted. Mongolia's government information exchange systems are based on the identification infrastructure which allows financial institutions to cross-verify proof of identity. Agents, the internet, mobile phones, ATMs, POS terminals are available for people to access digital financial services. Some financial institutions provide digital wallet services over their website and via applications. Financial institutions have started to use big data, data analytics, AI, process automatization, and blockchain technologies in their business processes.

RUSSIA - STATUS

POLICY

Russia has specific policies on identification, data protection, and KYC. Data protection and privacy are governed under the Law on Personal Data, which allows an individual to share his or her data held in State Information Systems with different financial organizations, with the consent of the individual concerned. This consent can be revoked as needed. Russia also has a focused strategy for financial inclusion. The Federal Financial Monitoring Service is an executive body that performs AML-CFT—related functions.

INFRASTRUCTURE

Russia has a strong penetration of identity cards with almost 100 percent of adults holding a national passport. Access to e-government services is provided through the Unified System of Identification and Authentication (USIA) introduced in 2011. The Central Bank of Russia has also developed the Unified Biometric System which was merged with the USIA to provide KYC services as per AML-CFT laws. Russia takes a risk-based approach to KYC and applies different levels of identification and monitoring commensurate with the risk profile of individuals. For the development of remote services, the Bank of Russia together with the Ministry of Digitization has conducted a pilot project, Digital ID (digital profile), based on the USIA. This provides citizens the possibility to manage their data from different sources, and to transfer their data at the request of a financial organization to obtain remote services through e-KYC. However, despite the introduction of e-KYC, there remains scope to reduce some of the challenges and delays caused by information missing from the identification system.

ECOSYSTEM

Russia has introduced a dedicated financial inclusion strategy with a focus on building digital channels and ICT infrastructure in remote and far-flung areas. It has a strong last-mile infrastructure and a variety of digital channels to expand financial services in remote areas. The Bank of Russia has also introduced a regulatory sandbox to allow the testing and development of model processes of new financial products, services, and technologies, which require regulatory changes.

TAJIKISTAN - STATUS

POLICY

Tajikistan has specific policies and guidelines on identification and data protection. Tajikistan guarantees the right to personal data protection in its constitution, which states that the collection, storage, use, and dissemination of personal data of an individual without his or her consent is prohibited.

INFRASTRUCTURE

Tajikistan issues an identity card for its citizens and has also replaced the conventional passport with a biometric-based passport. The government now has a unique database of a wide range of ID documents. Tajikistan does not have a digital identification system even though IDs and passports are issued. The KYC process is not yet used to remotely open e-wallets, and legal reforms are ongoing to ensure e-KYC can be used to open bank accounts and obtain loans with financial institutions. This will also make possible the implementation of simplified CDD measures for individuals who are of low AML-CTF risk.

ECOSYSTEM

Tajikistan has an inter-ministerial coordinating body that interacts with the central bank and various government ministries and departments but faces challenges of limited coordination and information exchange within government departments.

The financial literacy of the population is relatively low. However, the government and central bank are working actively to promote financial literacy and the launch of several financial literacy initiatives in the country is expected to improve the situation significantly. Internet services in Tajikistan have limited access and are highly priced, especially in remote areas. Limited use of the internet has slowed down economic development, including the growth of the financial sector.

UZBEKISTAN - STATUS

POLICY

The country's draft measures for issuing ID cards have been posted for discussion on the regulation.gov.uz portal. In 2019, Uzbekistan introduced its data protection law to regulate the protection of personal data.

INFRASTRUCTURE

Uzbekistan will soon introduce a unified personal identification system to replace the current biometric passport with an ID card linked by an electronic data carrier. The next step for the country is to develop and prioritize a national AML-CFT strategy. The risk assessment conducted by FATF recommended the implementation of a national customer identification and verification system, the implementation of compliance procedures as well as the organization of specialized training for investigators and judges on AML-CFT.

ECOSYSTEM

KYC is conducted using physical verification by bank branches, agents, offices of payment organizations, etc. e-KYC is not yet implemented in the country. The relevant government organizations are, however, developing a legislative framework as a basis for the implementation and operation of e-KYC. The Central Bank of Uzbekistan with the technical assistance of the World Bank has developed a draft NFIS. Its five pillars are:

- Increasing outreach of basic financial services
- Developing digital financial channels
- Enhancing SME finance
- Strengthening consumer protection
- Improving financial literacy

Several measures have been taken to increase financial inclusion. In particular, the number of electronic telecommunications devices, such as terminals, ATMs, and info kiosks, which form the basis of the infrastructure of payment systems, has been significantly increased. Along with this, contemporary technologies, such as QR codes and NFC, have been introduced, which facilitate the process of accepting and making payments without requiring expensive equipment.

The country faces some financial inclusion challenges such as limited concentration of financial services providers in remote areas, low financial literacy, and low utilization of mobile channels.

The principles of gender equality are taken into account in creating and maintaining financial inclusion policies. Also, every person, regardless of gender, has the same opportunities to access financial services.

According to a survey conducted by the International Finance Corporation in Uzbekistan in 2020, the country's gender gap is fairly low, at only 3 percent.[18]

METHODOLOGY

An extensive survey was conducted with the AFI member countries in ECAPI to gauge the status, opportunities, and challenges in the design and implementation of e-ID and e-KYC. A follow-up survey using an analysis framework (please see, below) was conducted to understand the supporting policies, infrastructure, and financial inclusion in the region.

The survey results were complemented by extensive literature review and secondary research. The summary of the results was collated and synthesized into guiding principles and situational analysis for each country. The regional framework on e-ID[19]and e-KYC will also complement AFI's existing policy model on e-KYC and digital ID and will advance financial inclusion by informing the development of e-ID and e-KYC in the EECA region.

Country-wise participation	Survey on e-ID and e-KYC	Analysis framework
Armenia	✔	✔
Belarus	✔	
Kazakhstan		
Mongolia	✔	✔
Russia	✔	✔
Tajikistan	✔	
Uzbekistan		✔

ANNEX 2: ANALYSIS FRAMEWORK

The analysis framework was used to capture the status of policies, infrastructure, and supporting ecosystem on e-ID and e-KYC of AFI member countries in the EECA region. The country-wise status shown above is largely based on the responses received for the analysis framework. The analysis framework captures information on three broad categories: policy, infrastructure, and ecosystem.

SECTION 1: POLICY

1.1 ELECTRONIC IDENTITY (E-ID)

I. What are the laws and policies around the national identity program (electronic Identity/ hard copy)? What are the details in the law or policy around:
   a. Is it mandatory for everyone to enroll in the identity program? If yes, at what age?
   b. What is the eligibility to get the identity document?
   c. Is it necessary to collect the biometric information of an individual to enroll them into the national identity program, and if so, what biometric information does it capture? (fingerprints, iris, etc.)?
   d. Does the law mention what Personal Identifiable Information (PII) and demographic data may be collected?
   e. What are the guidelines to make corrections, amendments, or deletion of inaccurate information in the identity card?
   f. Are there any update procedures for those whose biometrics are subject to change due to age or profession?

II. Which bodies of authority regulate Identity, digital ID, and collection of biometric data, and data protection? What are their key roles and responsibilities?

III. Which of the major government and private institutions have access to the identity database?

IV. What are the policies to access national identity information? Do third parties/ intermediaries have the authority to access the identity database for authentication purposes?

1.2 DATA PROTECTION

1. What are the guidelines, directives, or laws that exist on the processing of personal data of individuals?
   a. Is consent mandatorily required for processing data
   b. Are there any special provisions for children and vulnerable groups?
   c. Privacy by design principles imposed on data fiduciaries? (Limitations on collection of personal data, the period for which data can be retained)
   d. Conditions under which governments and private entities can access this data?
   e. Classification of sensitive data

2. Are there protections in place to limit access to the digital trail of personally identifiable information?

1.3 KYC AND AML-CFT

3. Do banking companies, financial institutions, and intermediaries face any challenges related to complying with KYC requirements and AML-CFT regulations?

4. Does the country allow tiered or risk-based KYC? What are the levels and tiers for KYC of individuals?

5. Which companies are mainly involved in providing e-KYC and AML-CFT verification services? What is the process followed? Who authorizes these entities?

SECTION 2: INFRASTRUCTURE READINESS

2.1 FOUNDATIONAL OR FUNCTIONAL IDENTITY

6. How much is the coverage of the national identity/ most common functional ID?
   a. What is the process for onboarding? Are there any direct costs involved for the citizens to onboard to the identity system? What are the costs for obtaining a birth and death registration?
   b. What is the process for onboarding typically excluded groups, such as vulnerable groups, refugees, and forcibly displaced people? Any special measures to provide online and offline registration service to the last mile in the remote and rural areas?
   c. For access to which services/ benefits (pensions, social assistance transfers, etc.) is the national identity card/number mandatory?

7. How is the accuracy of the data checked? Which databases are linked with the identity database? (e.g. national identity and civil registration)

8. What is the type of access (to the national identity database) given to various stakeholders (financial institutions, public bodies)? What are the different channels they can connect through (e.g. APIs)? What are the costing structures in place for this access (e.g. tiered costing)?

9. In which year was the system implemented? What are the features of the system? Can it perform deduplication, real-time updates?

10. How are laws on data privacy and consumer protection implemented and safeguarded through identity system design?
    a. How is customer consent taken into account? How are people given control over how their data is shared and processed?
    b. What are the measures in place for grievance resolution with respect to enrolment, and usage, in the identity program.

2.2 E-KYC INFRASTRUCTURE

11. Is e-KYC being implemented in the country? If yes, how? If no, are there plans to implement? What changes are required to implement e-KYC in the country?

12. What are the existing e-KYC practices (bank branch-based, agent-assisted, remote KYC, offline, etc) in the country? What is the rate of transactions?

13. What are the available modes for authentication (e.g. proof of identity and proof of address)?

14. What major risks and challenges do service providers face in the e-KYC process?

15. What are the exception handling procedures in place (e.g. biometric authentication failure in the case of remote onboarding requirements and other innovations)?

16. What are the use cases for e-KYC in enhancing financial inclusion in the country?

17. Which companies are mainly involved in providing e-KYC and AML-CFT verification services? What is the process followed? Who authorizes these entities?

SECTION 3: FINANCIAL INCLUSION STATUS

3.1 STRATEGIES AND INITIATIVES

18. Is there a financial inclusion governing body in the country? Is there a national financial inclusion strategy in place?

19. What are the existing financial inclusion challenges (e.g. lack of necessary documentation, non-availability of financial institutions in remote areas, cost of service, etc)?

20. What major initiatives have been taken to boost financial inclusion in the country? Any specific measures to advance financial inclusion to the poor and vulnerable?

21. How does electronic identity help resolve some of these challenges?

22. Is there a gender gap in financial inclusion status? What are the underlying reasons, and plans to address it?

23. Are there any products or services targeted to vulnerable groups (e.g. minimum or zero balance accounts)?

24. What has been the role of FinTechs in accelerating financial inclusion? Any specific guidelines to encourage FinTechs (e.g. regulatory sandbox)?

25. What channels (mobile phones, retail point of sales, agent banking, etc.) and instruments (wallets, digital financial services) are available for people to avail of digital financial services?

REFERENCES

Besides the policy documents of AFI member countries in the EECA region, the following are other sources referred to for the development of this policy framework:

1. AFI. 2020. Policy Model for National Financial Inclusion Strategy. AFI. Available at: https://www.afi-global.org/publications/policy-model-for-national-financial-inclusion-strategy/

2. The World Bank, ID4D. (Undated.) Practitioner's Guide: Types of ID Systems. Washington, DC: World Bank. Available at: https://id4d.worldbank.org/guide/types-id-systems

3. International Bank for Reconstruction and Development / World Bank. 2018. Catalog of Technical Standards for Digital Identification Systems. Washington, DC: World Bank. Available at: https://olc.worldbank.org/system/files/129743-WP-PUBLIC-ID4D-Catalog-of-Technical-Standards.pdf

4. AFI. 2021. Guideline Note on Digital Financial Services. AFI. Available at: https://www.afi-global.org/publications/guideline-note-on-data-privacy-for-digital-financial-services/

5. AFI. 2018. Gender Considerations in Balancing Anti-Money Laundering. Guideline Note No. 31. AFI. Available at: https://www.afi-global.org/wp-content/uploads/publications/2018-11/AFI%20GSP_laundering_stg7.pdf

6. World Bank. 2019. ID4D Practitioner's Guide: Version 1.0. Washington, DC: World Bank. Available at: http://documents1.worldbank.org/curated/en/248371559325561562/pdf/ID4D-Practitioner-s-Guide.pdf

7. AFI. 2019. KYC Innovations, Financial Inclusion and Integrity. Guideline Note No. 32. AFI. Available at: https://www.afi-global.org/sites/default/files/publications/2019-03/KYC-Innovations-Financial-Inclusion-Integrity-Selected-AFI-Member-Countries_0.pdf

8. Centre for Internet and Society. 2020. Governing ID: Principles for Evaluation. Bengaluru; Delhi: Centre for Internet and Society. Available at: https://digitalid.design/docs/CIS_DigitalID_EvaluationFrameworkDraft02_2020.01.pdf

9. Eurasian Group on Combating Money Laundering and Financing of Terrorism. 2018. Mutual Evaluation Report of the Republic of Tajikistan. Moscow: EAG. Available at: http://www.fatf-gafi.org/media/fatf/documents/reports/mer-fsrb/Mutual-Evaluation-Report-Republic-Tajikistan-2018.pdf

Alliance for Financial Inclusion
AFI, Sasana Kijang, 2, Jalan Dato' Onn, 50480 Kuala Lumpur, Malaysia
t +60 3 2776 9000 **e** info@afi-global.org www.afi-global.org
Alliance for Financial Inclusion AFI.History @NewsAFI @afinetwork