FIGI

FINANCIAL INCLUSION
GLOBAL INITIATIVE

SECURITY, INFRASTRUCTURE AND TRUST WORKING GROUP

e-KYC use cases in digital financial services

REPORT OF SECURITY WORKSTREAM

SECURITY, INFRASTRUCTURE AND TRUST WORKING GROUP

e-KYC use cases in digital financial services

DISCLAIMER

The Financial Inclusion Global Initiative (FIGI) is a three-year program implemented in partnership by the World Bank Group (WBG), the Committee on Payments and Market Infrastructures (CPMI), and the International Telecommunication Union (ITU) funded by the Bill & Melinda Gates Foundation (BMGF) to support and accelerate the implementation of country-led reform actions to meet national financial inclusion targets, and ultimately the global 'Universal Financial Access 2020' goal. FIGI funds national implementations in three countries – China, Egypt and Mexico; supports working groups to tackle three sets of outstanding challenges for reaching universal financial access: (1) the Electronic Payment Acceptance Working Group (led by the WBG), (2) The Digital ID for Financial Services Working Group (led by the WBG), and (3) The Security, Infrastructure and Trust Working Group (led by the ITU); and hosts three annual symposia to gather national authorities, the private sector, and the engaged public on relevant topics and to share emerging insights from the working groups and country programs.

This report is a product of the FIGI Security, Infrastructure and Trust Working Group, led by the International Telecommunication Union.

The findings, interpretations, and conclusions expressed in this work do not necessarily reflect the views of the Financial Inclusion Global Initiative partners including the Committee on Payments and Market Infrastructures, the Bill & Melinda Gates Foundation, the International Telecommunication Union, or the World Bank (including its Board of Executive Directors or the governments they represent). The mention of specific companies or of certain manufacturers' products does not imply that they are endorsed or recommended by ITU in preference to others of a similar nature that are not mentioned. Errors and omissions excepted; the names of proprietary products are distinguished by initial capital letters. The FIGI partners do not guarantee the accuracy of the data included in this work. The boundaries, colours, denominations, and other information shown on any map in this work do not imply any judgment on the part of the FIGI partners concerning the legal status of any country, territory, city or area or of its authorities or the endorsement or acceptance of such boundaries.

About this report

This report was prepared based on the inputs of the members of the Security, Infrastructure and Trust WG and contributions received from Vinod Kotwal, Department of Telecommunications, Ministry of Communications, India; Abbie Barbir, Co-rapporteur Question 10 ITU-T Study Group 17; Jason Burnett, Digital Trust; Rehan Masood, State Bank of Pakistan; Matthew Davie, KIVA.

If you would like to provide any additional information, please contact Vijay Mauree at tsbfigisit@itu.int.

Contents

LIST OF TABLES AND FIGURES

Tables

Figures

Executive Summary

Digital identity verification is rapidly growing as a direct result of digital transformation initiatives and has seen increasing growth due to the COVID-19 pandemic. Account opening is moving online, and service providers demand a secure and safe method to verify identity and for e-KYC. The main objectives of this report is to undertake an analysis of the technological innovations for e-KYC and compare the different approaches countries have adopted to implement e-KYC and provide information about technical standards that could be implemented to achieve interoperability at the level of the digital identity verification process. Use cases in India, Pakistan, and Sierra Leone are considered as well as new approach the Accountable Digital Identity Association (ADIA).

In India, earlier for issuance of Mobile SIM, a Customer Application form along with physical copies of Proof of Identity, Proof of Address and photographs were required. Management of physical record and wastage of paper was a big challenge. The Government of India through Department of Telecommunication is leveraging the e-KYC and authentication features of Aadhaar for provisioning of new mobile connection/issuance of SIM card. Under the new procedure, Telecom Service Providers (TSPs) are leveraging the e-KYC feature of Aadhaar wherein after getting the customer's consent using his/her Aadhaar number along with Biometric based e-KYC, UIDAI is sending the Digitally signed and encrypted details of customer's Demographic details (name, complete address, date of birth, gender and photograph) along with Aadhaar number to Telecom Service Provider along with Date and time stamp.

The required demographic details of customers are now captured in Customer Application Form (CAF) by the TSP and stored in its database. Once all the fields as required in CAF are completed, TSPs are issuing the SIM to customer. This new process is not only leveraging the e-KYC feature but also saving a lot of paper and is a big step towards green Telecommunication in India.

In Pakistan, a Biometric Verification System that allows for data flows between the telecommunications provider's Customer Relationship Management (CRMs) systems and the National Database and Registration Authority is used for Issuance of New SIM, Issuance of Duplicate SIM or SIM Replacement, Change of Ownership, Mobile Number Portability (MNP) and Re-Verification (re-verification of existing active SIM). A verified customer SIM Card issued through the BVS system can be used for remote opening of Level 0 DFS accounts.

To ease remote account opening, Decentralized Identifiers (DID) can be adopted for the task of performing online identity verification, well-designed DID system can allow the user to conduct many identity-verification and authentication transactions over "zero-knowledge" protocols that mathematically prevent information leakage and can even thwart privacy-violation threats that arise from event correlation. Service Providers benefit from lower costs and a much higher level of assurance in every verification transaction, plus auditable verification proof that may be recorded to a distributed ledger.

One use case of the decentralized identifier using blockchain, is the Kiva Protocol, a network of nodes supporting a public decentralized identity (DID) registry which has been implemented in Sierra Leone. This registry provides the foundation of trust in the digital credentials used to verify identity. The KIVA protocol enables citizens to present and authenticate official digital identity credentials with financial institutions. citizens can securely share authenticated official identity credentials with the financial sector to support KYC and customer due diligence compliance.

The DID Alliance seeks to fulfil the promise of the DID systems by enabling a business interoperability layer as well as a technological one through the Accountable Digital Identity Association (ADIA). At the heart of ADIA is the Digital Address; the Digital Address is a special ADIA identifier issued to an individual by a certified Digital Address Issuer after Know Your Customer (KYC) processes have been followed.

Distributed ledger technologies can also allow persistent identifiers, in which the identities of their holders are likely to be cryptographically verified. This new type of verifiable and self-sovereign digital identities, where the control of them resides entirely in the hands of the users, regardless of any centralized registry, identity provider or certification authority are unique, global and portable for life.

There is a need for a technical standard which defines a framework for decentralized identity management aimed at individuals for e-KYC purposes for remote onboarding to provide interoperable and

trusted solutions. The technical requirements for this standard is discussed in section 7 of the report and its main components includes the relationship of the main participating entities, the interactions during the decentralised ID lifecycle for the issuance, delivery and receipt of the verifiable credentials. Such a standard could facilitate the deployment of such technologies and promote interoperability among the various platforms that are used for such authentication mechanism.

Acronyms

ADIA	Accountable Digital Identity Association
AEPS	Aadhaar Enabled Payment System
AML	Anti-Money Laundering
APB	Aadhaar Payment Bridge
API	Application programming Interfaces
ASA	Authentication Service Agency
ASP	Application Service Provider
ATM	Automated Teller Machine
AUA	Authentication User Agency
BC	Business Correspondents
BHIM	Bharat Interface for Money
CA	Certifying Authority
CCA	Controller of Certifying Authority
CIDR	Central Identities Data Repository
CSR	Certificate Signing Request
DAP	Digital Address Provider
DBBR	Database containing Biometric Reference
DBIR	Database containing Identity Reference
DBT	Direct Benefit Transfer
DID	Decentralized Identifier
DIDA	DID Alliance
DIF	Decentralized Identity Foundation
DLT	Distributed Ledger Technology
DLTS	Digital Locker Technical Specifications
DOT	Department of Telecommunication
DSC	Digital Signature Certificate
e-KYC	Electronic-Know Your Customer
ESP	eSign Service Provider
FIDO	Fast IDentity Online – open authentication standard
FP	Fingerprints
HSM	Hardware based Security Module
IBA	Indian Banks Association
IMPS	Immediate Payment Service

MeitY	Ministry of Electronics & Information Technology
NACH	National Automated Clearing House
NFS	National Financial Switch
NPCI	National Payments Corporation of India
NUUP	National Unified USSD Platform
OTP	One Time Password
PDS	Public Distribution System
PID	Personal Identity Data
PKI	Public Key Infrastructure
PSP	Payment System Players
RBI	Reserve Bank of India
RD	Registered Device
SSL	secure socket layer
STQC	Standardisation Testing and Quality Certification
UIDAI	Unique Identification Authority of India
UPI	Unified Payment Interface
URI	Uniform Resource Indicator
USSD	Unstructured Supplementary Service Data
VC	Verifiable Credential
VPA	Virtual Payment Address
W3C	World Wide Web Consortium

Glossary

Credential Wallet – a piece of software (or other embodiments) that is capable of securely storing digital credentials – usually a mobile phone app.

Decentralized Identifiers (DIDs) – A portable URL-based identifier, associated with an entity. These identifiers are most often used in a credential and are associated with subjects such that a credential itself can be easily ported from one repository to another without the need to reissue the credential. An example of a DID is did: example:123456abcdef.

Digital Address – A special ADIA identifier that is issued to an individual by a ADIA-certified Digital Address Issuer after a KYC process.

Digital Address Provider (DAP) (Role) – a solution or service provider that uses DID technology to manage distributed identity data for users in the ADIA ecosystem.

Distributed Ledger (DLT) – A distributed ledger is a database that is consensually shared and synchronized across multiple sites, institutions, or geographies. It is often embodied as a blockchain.

FIDO – the strong authentication specification managed by FIDO Alliance.

ADIA – Accountable Digital Identity Associationprovides trust sourcing, cross-ledger transaction enablement for distributed ledgers and inclusiveness for all types of users.

KYC – "Know Your Customer": a process in which an agent of an organization performs certain due diligence to establish the positive identity of a user or claimant. When this is done using an online system or online-enabled tools it is referred to as **e-KYC**.

Service Provider (Role) – a relying party in the ADIA ecosystem; consumes Verifiable Credentials.

Verifiable Credential (VC) – A verifiable credential can represent all of the same information that a physical credential represents. The addition of technologies, such as digital signatures, makes verifiable credentials more tamper-evident and more trustworthy than their physical counterparts. A specification is managed by W3C.

E-KYC use cases in digital financial services

1 INTRODUCTION

Lack of legal identification is a major challenge to financial inclusion. Digital identity management solutions can make identity easier to manage and access and therefore can play an enabling role in enhancing financial inclusion. Emerging technologies, biometric data, distributed ledgers, and artificial intelligence are enabling new solutions for e-KYC. e-KYC leverages these technologies to create new approaches that are more cost-efficient and effective. Stakeholders in both public and private sectors are developing innovative solutions based on these technologies to discharge their due diligence responsibilities.

In digital financial services, customer identification and verification are key elements of the customer due diligence process. The term KYC (know your customer) refers only to the customer identification and verification elements of customer due diligence. KYC registries are services that store customer identity data in a single repository for use by multiple financial service providers.

The financial service provider must verify the customer's identity using reliable, independent source documents or data available. In the case of unbanked customers, this verification may not be always possible this could be a barrier to financial inclusion. In this context, a tiered KYC may be justified, but this is not always an option as the risks must first be assessed and compared against the likely benefit of the relationship to the provider. Digital identity management solutions can be combined with tiered KYC to better address these challenges.

In some countries the public sector plays a role to support the digital identity verification process for the DFS providers. In this context, usually national identity authorities provide the infrastructure for digital identity verification and are an important stakeholder in the e-KYC process. Examples are India, Pakistan, Malaysia, Sierra Leone, and Singapore with e-KYC initiatives by the public sector.

The main objectives of this report are to undertake an analysis of the technological innovations for e-KYC and compare the different approaches countries have adopted to implement e-KYC and provide information about technical standards that could be implemented to achieve interoperability at the level of the digital identity verification process.

2 INDIA

In India, the Aadhaar program, provides a unique identifier (a random 12-digit number) to the residents. A DFS provider can verify a customer's identity using the customer's Aadhaar number and a fingerprint and/or iris scan. DFS providers rely on the results of Aadhaar authentication without further identity verification, thus simplifying the customer due diligence process for them.

In September 2018, the Supreme Court of India ruled that a section of the Aadhaar Act related to private sector use of e-KYC was unconstitutional. This resulted in private sector access to e-KYC services not being offered. e-KYC use for public services, such as social assistance payments, was not affected, and continued to be available. To allow use of e-KYC by the private sector, a regulation was adopted in 2019 allowing particularly, DFS providers and telecommunication companies, to use e-KYC.

2.1 India Stack

Building on the Aadhaar functionality, the India Stack has open and programmable capabilities with four distinct layers:

- **A presenceless layer** where a universal biometric digital identity allows people to participate in any service from anywhere in the country.
- **A paperless layer** where digital records move with an individual's digital identity, eliminating the need to collect and store massive amount of paper.
- **A cashless layer** where a single interface is available to all the country's bank accounts and digital wallets.
- **A consent layer**, which allows user data to move efficiently and securely, based on user consent and control.

Each layer of the stack is built on a specific technology intervention as indicated below:

Table 1: India Stack

Layer	Feature	Technology intervention
Presenceless	Unique digital biometric identity	Aadhaar authentication
Paperless	Rapidly growing base of paperless systems with billions of artefacts	Aadhaar e-KYC, ESign & Digilocker
Cashless	Game changing electronic payment systems facilitating transition to cashless economy	IMPS, Aadhaar Payment Bridge (APB), Aadhaar Enabled Payment Services (AEPS) & Unified Payment Interface (UPI)
Consent	Provides privacy data sharing framework	Corresponding public APIs under open API policy

The data flowing through the various layers of India stack can be tracked digitally, providing traceability. Thus, India stack has ushered in a new era in delivery of services adhering to the principles of governance viz., being participatory, transparent, accountable, responsive, effective and efficient.

Building on India stack to deliver financial services/facilitating digital payments.

- Aadhaar as an ID authentication to enable electronic KYC and opening of customer accounts at very low cost/friction.
- Aadhaar as an ID authentication for transactions.
- Aadhaar as a financial destination – so send money to Aadhaar number instead of Bank Account/ IFSC Code using NPCI's UPI platform.

2.2 Unique Identification Authority of India (UIDAI)

The authority responsible for issuing the Aadhaar number is the Unique Identification Authority of India (UIDAI). UIDAI has been tasked with three key functional processes: enrolment, identification, and authentication. Through an extensive network of enrolment agencies, UIDAI collects the demographic (name, date of birth, gender, address) and biometric (fingerprints, iris scan and photograph) information

from individuals for the purpose of enrolling them into the Aadhaar system.

The biometric and demographic data is maintained in a Central Identities Data Repository (CIDR), identity claims and authentication services are provided through open Application Programming Interfaces (APIs) with yes/no answers. Several applications like eSign, digital locker, mobile banking apps etc. use Aadhaar biometric based authentication services.

UADAI provides the following functional processes to enroll and verify identity of users of Aadhaar

- **Enrolment process**: creating and storing an enrolment data record for an individual who is the subject of a biometric capture process in accordance with the enrolment policy. The subject usually presents his/her biometric characteristics to a sensor along with his/her identity reference. The captured biometric sample is processed to extract the features which are enrolled as a reference in the enrolment database with identity reference.
- **Verification process**: testing a claim that an individual who is the subject of a biometric capture process is the source of a specified biometric reference. The subject presents his/her identity reference for a claim of identity and biometric characteristic(s) to the capturing device, which acquires biometric sample(s) to be used for comparison with the biometric reference linked to the identity reference for identification. The verification process has a possibility of impacting a subject's information privacy, since this process requires both biometric reference and identity reference. The identification process requires exhaustive search of enrolment database. So, this also has a possibility of impacting on subject's physical privacy. Verification is generally considered to be less privacy intrusive than identification. In Aadhaar system verification is done via online authentication having only a "yes/no" answer.

2.3 National Payments Corporation of India

While Aadhaar system provide basic identity authentication, National Payments Corporation of India (NPCI), an umbrella organization set up with the guidance and support of the Reserve Bank of India (RBI) and Indian Banks Association (IBA) provides infrastructure to the entire Banking system for physical as well as electronic payment and settlement systems.

NPCI has collaborated with Unique Identification Authority of India (UIDAI) to create a centralised Aadhaar mapper. It maintains an association between customer's Aadhaar number, mobile number, and Bank accounts. This central repository can be used to route payment instructions based on Aadhaar number or mobile number. The Aadhaar mapper, at present acts as an enabler for payment owing to the Aadhaar number mapping to the Account number as the financial address. NPCI has already build capabilities such as the e-KYC and Aadhaar Payment Bridge (APB) system around this enablement. Unified Payment Interface (UPI), Immediate Payment System (IMPS), and National Unified USSD Platform (NUUP) can take advantage of Central Mapper for fetching and routing their payments. Hence having such a common repository can create a great process value add, for overall payment ecosystem and consequently to the end customer.

2.4 Authentication and e-KYC for DFS

UIDAI offers two types of services/facilities for private sector and DFS providers:

a) Authentication services to authenticate identity claim in the form of Yes/No using biometric or Mobile OTP; and
b) E-KYC (Electronic Know your Customer) authentication explicitly allowing UIDAI to share their demographic data with the requesting party only after Aadhaar holder's consent.

To explain how the authentication and e-KYC services work a brief overview of the Aadhaar authentication and KYC ecosystem is provided first, which, describes the role of each stakeholder.

2.4.1 Aadhaar authentication ecosystem

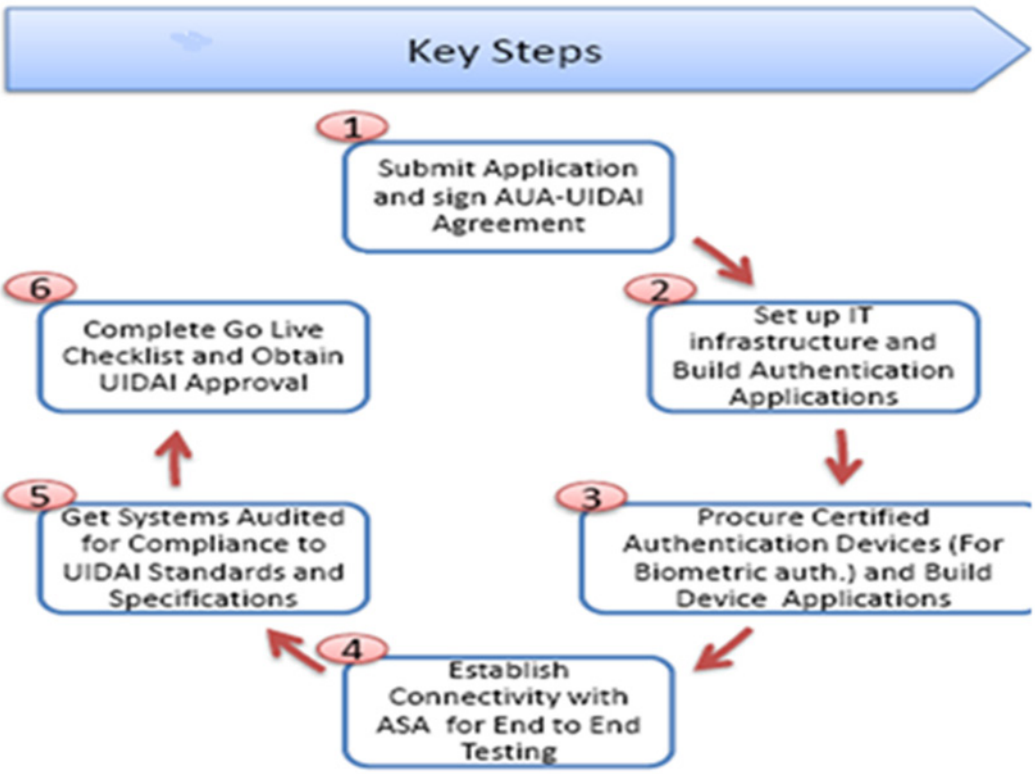
The Aadhaar authentication ecosystem has following agencies:

a) AUA (Authentication User Agency)

AUA connects to the Aadhaar Database and uses Aadhaar authentication to validate a user and enable its services. Examples of AUAs are banks, various state and central government ministries providing services such as the Public Distribution System (PDS), the National Rural Employment Guarantee Scheme (NREGS), and private agencies like mobile phone operators. An AUA is required to enter a

formal contract with UIDAI to be able to use Aadhaar authentication services (see Figure 2). Any other agency seeking to conduct Aadhaar authentication of its customers/associates etc. for service delivery can engage with an existing AUA and such agencies, which enter into agreements with AUA, are defined as Sub-AUA.

Figure 1: Department AUA on-boarding process



b) Authentication Service Agency (ASA)

ASA is any entity that transmits authentication requests to the Aadhaar database on behalf of one or more AUAs. They play the role of enabling intermediaries. They have an established secure connection with the Aadhaar database and convey authentication requests of more than one AUA thereto. ASAs receive the Aadhaar database response and transmit the same back to the AUA. An ASA may enter into a formal contract with AUAs. UIDAI has a set of guidelines that may be included in the contract between an ASA and an AUA. However, the contract (and commercial terms, if any) between an ASA and an AUA is at the sole discretion of the signing parties.

c) e-KYC User Agency (KUA)

A KUA is any entity, which uses Aadhaar authentication to enable its services and connects to the Aadhaar database through an ASA.

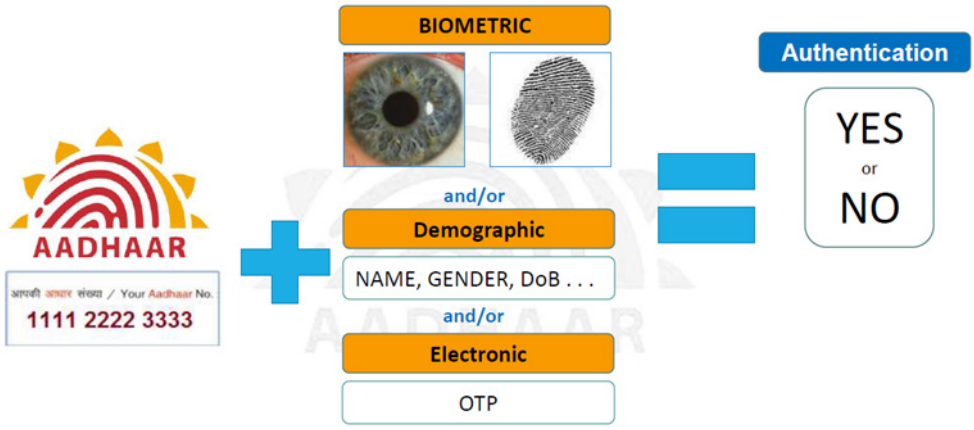
d) e-KYC Service Agency (KSA)

KSAs are entities with connectivity with the Aadhaar database and can share the demographic profile of the Aadhaar card holder with the KUAs for authentication purpose. Every KSA is also an ASA.

2.4.2 Aadhaar authentication and e-KYC

Aadhaar authentication is the process wherein the Aadhaar Number, along with other attributes, including biometrics, are submitted online to the Aadhaar database for its verification based on information or data or documents available with it. During the authentication, the person's record is first selected using the Aadhaar Number and then the demographic/biometric inputs are matched against the stored

Figure 2: Authentication Service



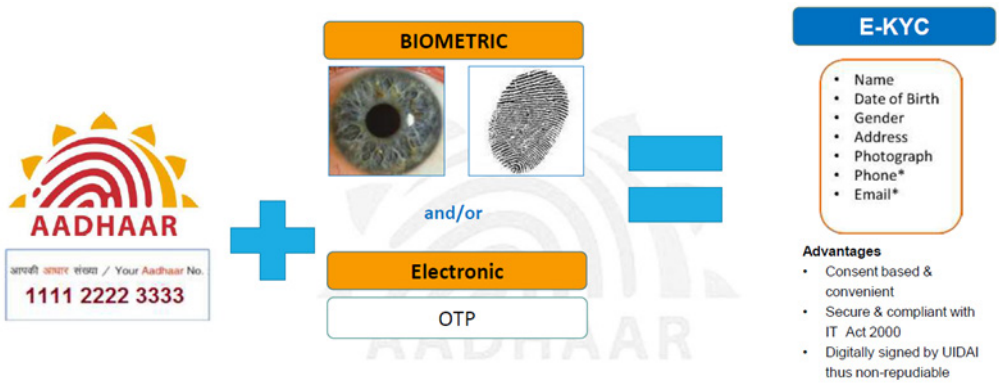
data, which was provided by the person during enrolment/update process. Alternatively, authentication can also be carried out based on the OTP.

The Aadhaar e-KYC service allows UIDAI to share electronic version of Aadhaar information (demographic information and photo ONLY) with the explicit consent of the person. During the e-KYC process, UIDAI encrypts the e-KYC response data containing the person's latest demographic and photograph information using KUA public key and forwards the encrypted response to KUA. On receiving the encrypted response, the KUA decrypts the data using their own private key and returns an XML with 7 pieces of data:- Name, Address, DOB, Gender, Phone number, email address and photograph, this eliminates collecting photocopy of Aadhaar letter from resident. All biometric or OTP authentication schemes are valid for e-KYC service.

2.5 Technical process of Authentication & e-KYC services

Authentication devices used by Authentication user agency/e-KYC user agency initiate the authentication request (Figure 2) and create encrypted PID (Personal Identity Data) block before forwarding it to authentication server of AUA/KUA for processing of domain specific transaction and creation of auth XML as per UIDAI authentication API. Further, upon receiving the auth XML from AUA, Authentication Service Agency (ASA) forwards it to CIDR. To ensure the integrity and non-repudiation, Authentication Server at CIDR, as a mandatory requirement, accepts only digitally signed auth XML through ASA.

Figure 3: Aadhaar e-KYC



The following are the major steps in Aadhaar authentication process as shown in Figure 4 below:

- Aadhaar holder sends the authentication request through the devices
- Aadhaar authentication enabled application software, which is installed on the device, encrypts, and sends the data to AUA server
- AUA server, after validation, adds necessary headers (AUA specific wrapper XML with license key, signature, etc.), and passes the request through ASA server to UIDAI CIDR.
- Aadhaar authentication server returns a "yes/no" based on the match of the input parameters.
- Based on the response from the Aadhaar authentication server, AUA/Sub-AUA conducts the transaction and Aadhaar holder receives the service.

2.6 Additional Security features for Authentication/KYC service

a) To further enhance the security of Aadhaar authentication eco-system, under Regulations 14(n) and 19(o) of Aadhaar (Authentication) Regulations, 2016, it is decided to mandatorily use Hardware Security Module (HSM) for digital signing of Auth XML and decryption of e-KYC data.

b) For digital signing of Auth XML, Authentication request is digitally signed by the requesting entity (AUA/KUA) and/or by the ASA using HSM, as per the mutual agreement between them. However, to decrypt the e-KYC response data received from UIDAI, the KUA shall necessarily use its own HSM.

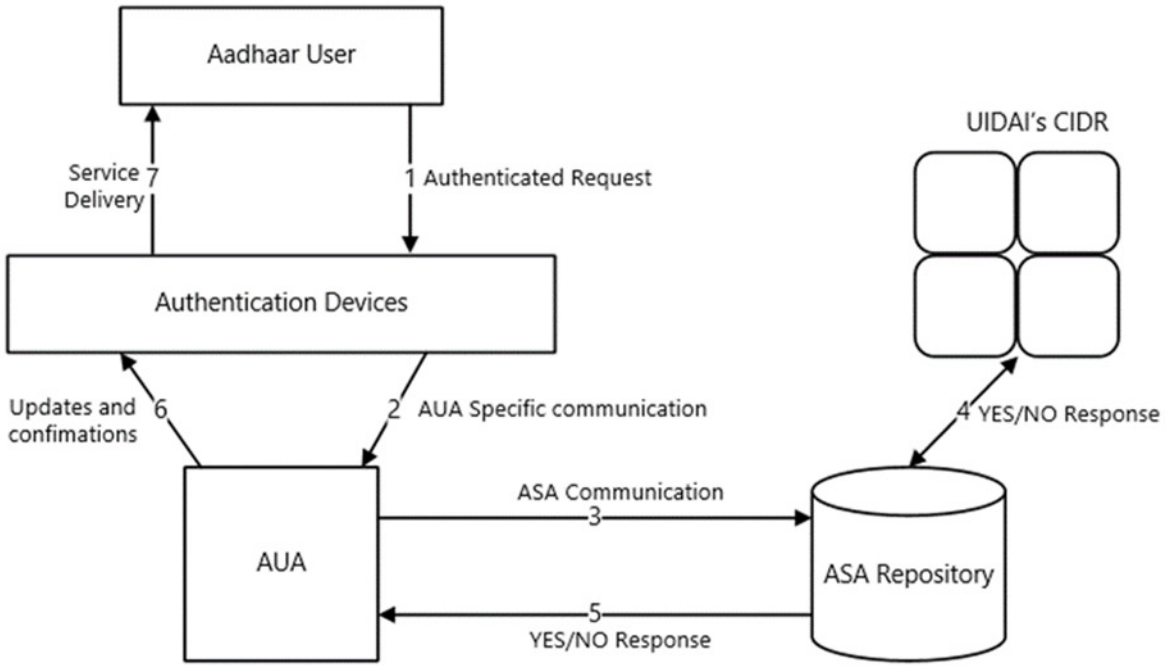
c) The HSM to be used for signing Auth XML as well as for e-KYC decryption is FIPS 140-2 compliant.

d) All AUA/ KUA/ASA ensures the implementation of HSM in Aadhaar authentication services.

e) To eliminate the use of stored biometrics, UIDAI has mandated the use of registered devices by AUA/KUAs and ASAs. The registered devices provide the following key additional features compared to public devices:

- Device identification – every device having a unique identifier allowing traceability, analytics, and fraud management.
- Eliminating use of stored biometrics – biometric data is signed within the device using the provider key to ensure it is indeed

Figure 4: Technical process of Authentication & e-KYC services



captured live. Then the Registered Device (RD) Service of the device provider must form the encrypted PID block before returning to the host application.

2.7 Integration of FIDO & Aadhaar: Merging Real Identity with Virtual identities

This section provides some indication as to how FIDO could be integrated with Aadhaar system in India.

FIDO (Fast Identity Online) is the World's Largest Ecosystem for Standards-Based, Interoperable Authentication with Google as the alliance president, Microsoft as the vice president with representation from major segments of the markets globally. FIDO's mission is to eliminate the reliance on network passwords, which is the major source of identity fraud and major source of pain for the common user. There are already major deployments of FIDO globally from financial organizations, to network operators to e-commerce service providers to cloud infrastructure providers. FIDO eliminates the most common identity fraud sources like phishing attacks, server-side attacks, man in the middle attacks, dictionary attacks and global attacks that are rampant.

W3C is making FIDO Authentication part of Web Authentication specification for browsers. There are already Mobile phones from all major mobile original equipment manufacturers like Apple, Samsung, Huawei, Lenovo for the past two years that are already FIDO capable. In the FIDO architecture, the root of trust for the identity is tied to a service that the user is logging in to. For the same user and same device, user device will have different public/private key.

For a country like India with a large population and a mobile based economy with big investment in centralised ID systems like Aadhaar, there is a good opportunity to design strong authentication systems that are based on the FIDO standard.

This could be done by building on the solid base that India has already built. It is very impressive to see how much Aadhaar is being embraced in the arena of KYC and linking the identity with Aadhaar. Real upside would be expanding the Aadhaar ID to provide a derived credential for Aadhaar verification into a user smart phone with an Identity service that would be in the cloud, that can be used for every transaction that a citizen performs at various places without really interacting with the Aadhaar database each time.

mAadhaar mobile application could be a perfect place to integrate FIDO and provide a cloud-based identity that is verified by Aadhaar. While mAadhaar is a great tool that authenticates offline, there would not be any audit trial or any other trace that can be recorded away from the user device. This would be an exposure for fraud and at the same time, and it cannot be in a non-operator assisted operation.

Under this approach, using an Identity Cloud (referred to as "AadhaarHub") that is tied to mAadhaar mobile app, any time, and every time a user needs to be authenticated, all user needs to do is to use FIDO to authenticate with mAadhaar app and the authentication validation is done on the identity cloud. This provides data privacy as there is no specific user information that is sent to the server other than FIDO assertion. The user biometrics never leaves the device, and the authentication can only happen on that device for that user and with the AadhaarHub.

This could also be a great vehicle to deliver government services to the citizens, enable peer-to-peer payments, and with simple tap and go, other payments in public transportation and other merchant locations with server-side authentication with high assurance on the identity.

mAadhaar and AadhaarHub can be part of the "India Stack" and in this way device manufacturers could be influenced to include in the software stack. This will provide the scale with every device that is sold in India without causing extra burden to the device manufacturers. And the "India Stack" can be the standard that would promote a userID, password less identity that can be offered to major service providers that are offering services to Indian citizens where there will be a binding between their virtual identities and real identity which will really help curb the cyber fraud.

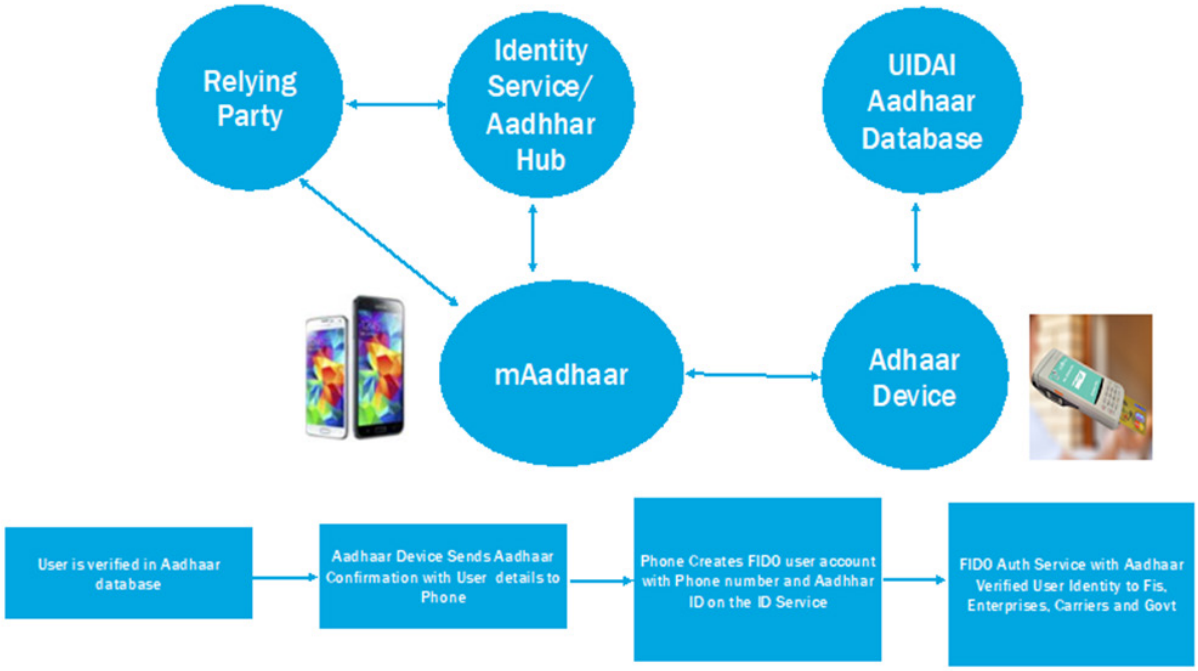
This could be a showcase for entire world how cybersecurity can and should be handled to provide the anonymity and privacy that is required in the cyber world that is safe, at the same time provide the enough identity assertion when solving a cybercrime.

3 PAKISTAN

3.1 Biometric Verification System (BVS)

The SIM sale procedures deployed prior to BVS initially performed well, however, demand for illegal SIMs, especially for illegal international traffic termination (SIM box) paved the way for a system bypass. Publication of electoral rolls and their access to public for 2013 general elections indirectly provided access of

Figure 5: ID proofed Auth server: No User ID



secret information i.e., mother's name and place of birth against CNIC of the general public and fraudsters made effective use of it for identity theft in an organized manner. Hence, need was felt to evolve a secure SIM issuance system which could provide "proof of life".

3.2 BVS Data Flow

In BVS, data flows from the sale channel to NADRA database through CMOs Customer Relationship Management (CRMs) systems in following steps:

a) When a potential subscriber visits a sale channel for a SIM related transaction, the sale agent asks his/her CNIC number, punch-in mobile number, scans thumb/finger and sends the data (CNIC number and biometric information template) to the mobile operator.
b) The systems at mobile operators' end checks eligibility of the sale channel (through its unique ID), eligibility of the subscriber (i.e., count of SIMs is less than five) and if eligible, forwards the information to NADRA.
c) NADRA checks validity of CNIC and matches the received information in its database. Success or failure is returned to the mobile operator based upon the verification result along with data (Name, Father's name, address), if requested by the CMO.
d) Received data is used to update the system and subsequently the result is forwarded to sale channel's device.
e) In case of successful verification, SIM is handed over to the customer whereas in case of failure, further guidance is provided based upon the error code generated by NADRA.

3.3 Salient Features of BVS

BVS is a fully automated process with minimal human intervention with the following salient features:

3.3.1 BVS process

The inputs include Computerized Identity Card (CNIC) number, finger index (Right Thumb, Right Index, Left Thumb, Left Index) and finger impression. In output, we get the verification result (i.e., Success/ Failure) and subscribers' data (Name, Father's Name, Address), if required.

3.3.2 BVS devices

There are three types of devices used in the process:

a) Microsoft Windows based personal computer with a finger/thumb scanner which is connected

Figure 6: Aadhaar proofed derived identity

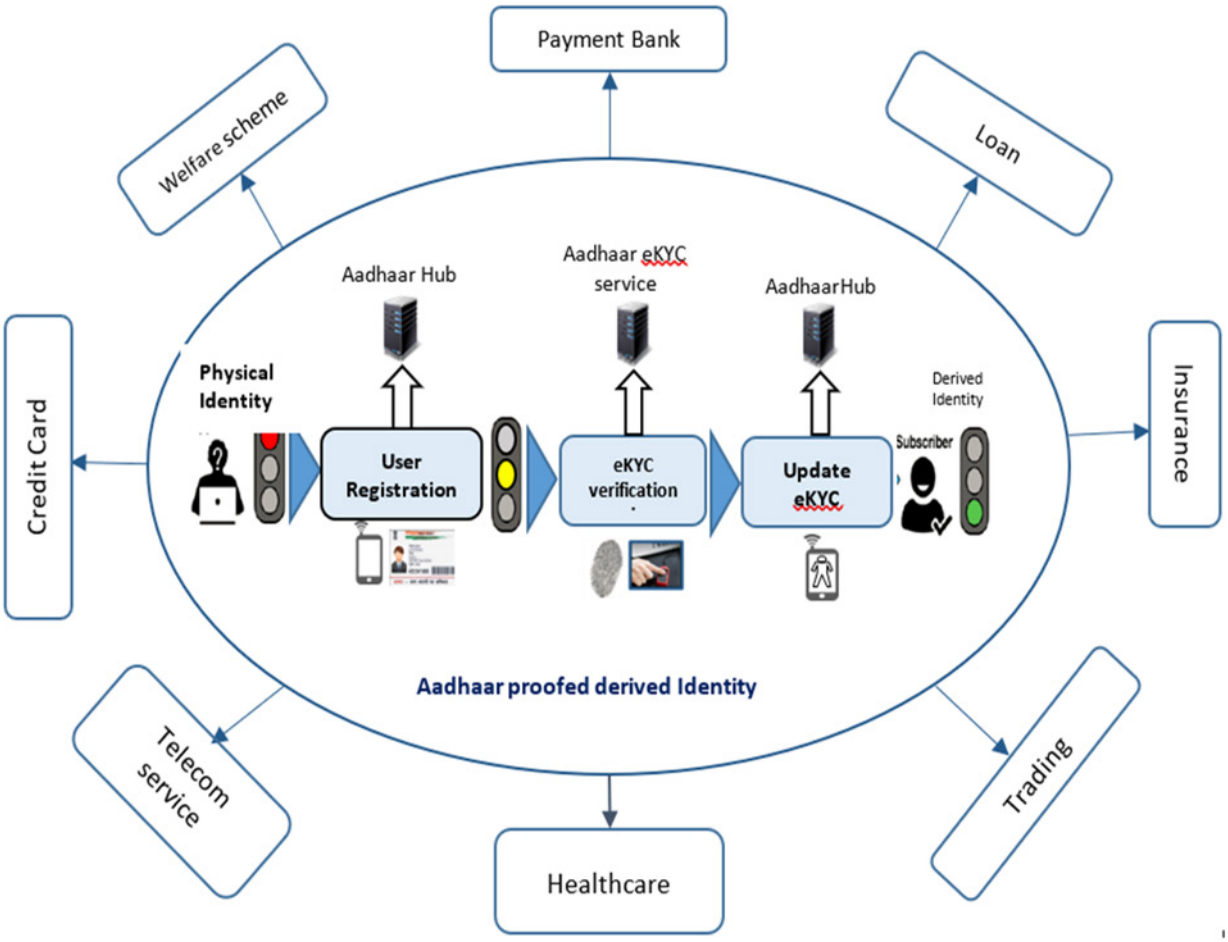
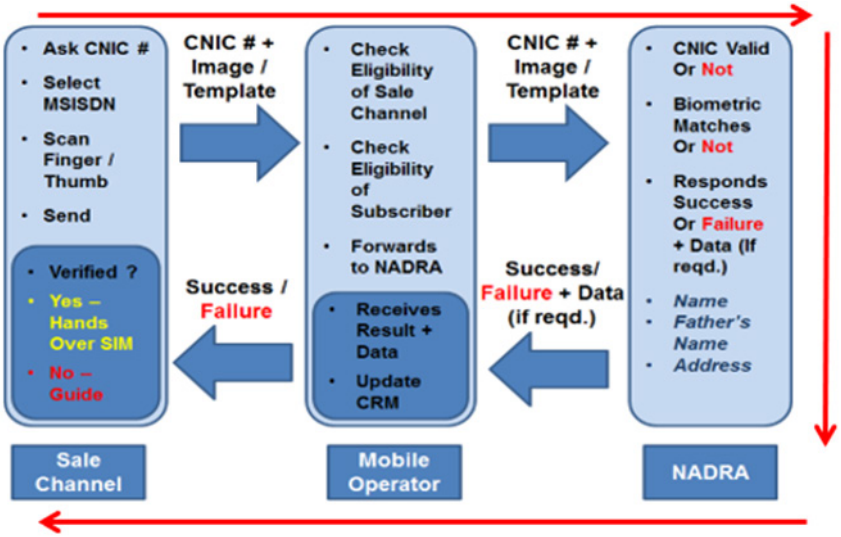


Figure 7: BVS Data Flow



to the PC through USB. The PC hosts an application which captures finger impressions and communicates the information to the mobile operator. This solution is mostly used at Customer Service Centres (CSCs) and Franchisees which usually have a fixed premise and a power backup.

b) Specialized Android based terminals and Android tablets with finger scanners (Figure 2) have been deployed mostly at retail level.
c) In some circumstances, the process is also carried out through a blue tooth enabled phone and finger scanner.

The devices are connected to the databases via VPNs over Internet and the access is arranged through Digital Subscriber Line (DSL) or Edge/GPRS or Mobile Broadband (3G/4G) depending upon the type of device and service area.

3.3.3 BVS Transactions

Currently, following transactions are carried out through BVS:

a) Issuance of New SIM.
b) Issuance of Duplicate SIM (SIM Replacement or Change of SIM).
c) Change of Ownership (Changing Ownership from one owner to another).
d) Mobile Number Portability (MNP).
e) Disowning (disowning a SIM registered on a CNIC).
f) Re-Verification (re-verification of existing active SIM).

3.3.4 Data Source & Image Format

Verification of biometric information is real-time which is done from NADRA (the national database of Pakistan having biometric information). A unique transaction ID is assigned to each transaction for tracking and audit purposes. The biometric information for verification is required to be captured at at-least 500 dpi and the supported standards for image acquisition are Pkmat, ANSI 378 and ISO 19794.

3.3.5 Technical Standards

NADRA is the custodian of Pakistani citizens' data. For verification purposes, they have exposed a web API for telcos which supports following standards for interacting with NADRA's AFIS:

a) Pkmat
b) ANSI 378
c) ISO/IEC 19794-2
d) Fingerprints are sent to NADRA as a Template or Image (WSQ/JPG/BMP) as per any of the supported standard used by a telco.
e) Fingerprints are available at NADRA's database. One to one matching of CNIC # and corresponding Fingerprint (image or template as per the used standard) sent by CMO is made at NADRA's end and response in the form of Success or Failure are sent back to CMO concerned.
f) Complete Packet encryption (AES 256bits) is used for encryption of data sent to CMOs and NADRA.

3.3.6 Biometric Verification for Branchless Banking

Without compromising the requirements of AML/CFT, the State Bank of Pakistan (SBP) has opted a risk-based approach to customers due diligence for branchless banking accounts. As per State Bank of Pakistan's Branchless Banking Regulations issued vide BPRD Circular No: 09 of 2016., Biometric Verification requirement for over-the-counter branchless banking transactions was made mandatory from July 01,2017.

The regulations are available at http://www.sbp.org.pk/bprd/2016/C9.htm Further, in line with the objectives of National Financial Inclusion Strategy 2015, the above mentioned regulations allowed remote opening of Level 0 accounts, however, it was required that account of a customer shall be opened against verified SIM Card. [Note: Via its BPRD Circular No. 18 of 2018, SBP has required banks to carry out biometric verification of the existing customers].

4 E-KYC USING DECENTRALIZED IDENTIFIERS

The main problem facing remote account opening is the task of performing online identity verification. Methods that enable the bootstrapping of trusted online identity vetting are required.

The concept of "self-sovereign" identity promises to mitigate or eliminate the problems of conventional identity-related interactions by placing the user in control of his or her own identity assets. A DID system consists of a set of tools and services that implement the self-sovereign identity concept.

Many DID systems are deployed on distributed ledgers. Ledgers provide various benefits, including:

a) Key management: The ledger significantly simplifies tasks traditionally associated with certification authorities and PKI systems.
b) Audit trail: Where needed, the ledger can record transaction proofs for legally or economically consequential events.
c) Economic model: The ledger can implement and enforce payment flows associated with identity-related transactions.

These technological tools can enable the user to manage his or her information and to decide exactly what is disclosed and under what circumstances. A well-designed DID system can allow the user to conduct many identity-verification and authentication transactions over "zero-knowledge" protocols that mathematically prevent information leakage and can even thwart privacy-violation threats that arise from event correlation.

Service Providers benefit from lower costs and a much higher level of assurance in every verification transaction, plus auditable verification proof that may be indelibly recorded to a distributed ledger.

Verifiable Credential Issuers can not only save substantial costs related to paper-credential issuance, but, owing to the payment-handling capabilities of distributed ledgers, can build entire new businesses based on incremental revenue accruing through use of their issued credentials.

The next sections examine two examples of decentralized ID system used for biometric registration and e-KYC.

5 SIERRA LEONE'S NATIONAL DIGITAL IDENTITY PLATFORM

Sierra Leone launched the National Digital Identity Platform (NDIP) in August 2019. The NDIP is an extensible digital identity infrastructure – built using Kiva Protocol's open source technology – that enables citizens to present and authenticate official digital identity credentials with financial institutions. Once fully integrated into the financial sector and supported by an appropriate regulatory regime, the NDIP will provide the foundation for a market wide e-KYC utility in Sierra Leone.

The NDIP leverages the identity data collected and held by Sierra Leone's National Civil Registration Authority (NCRA), a citizen registry created by the Government of Sierra Leone to support broad participation in the 2018 general elections. In partnership with the United Nations Development Programme (UNDP) and leveraging more than 2,500 identity registration sites across the country, the civil registration efforts leading up to the election yielded near-universal official identity coverage for Sierra Leone's adult population.

Working with Kiva, a US-based nonprofit focused on financial inclusion, the NDIP has helped migrate the identity data in the NCRA database into verifiable credentials held by citizen-controlled and -permissioned digital wallets. As the NDIP wallet infrastructure is integrated into the financial sector, any adult citizen with an NCRA-issued identity credential will be able to securely authenticate their official identity with FSPs to support e-KYC for new account opening and ongoing customer due diligence (CDD).

5.1 Kiva Protocol – System Overview

The Kiva Protocol implementation in Sierra Leone has a three-layer architecture to enable citizens to securely share authenticated official identity credentials with the financial sector to support KYC and CDD compliance.

5.1.1 Public utilities

The foundation of Kiva Protocol is a network of nodes supporting a public decentralized identity (DID) registry. This registry provides the foundation of trust in the digital credentials used to verify identity.

5.1.2 Trusted connections

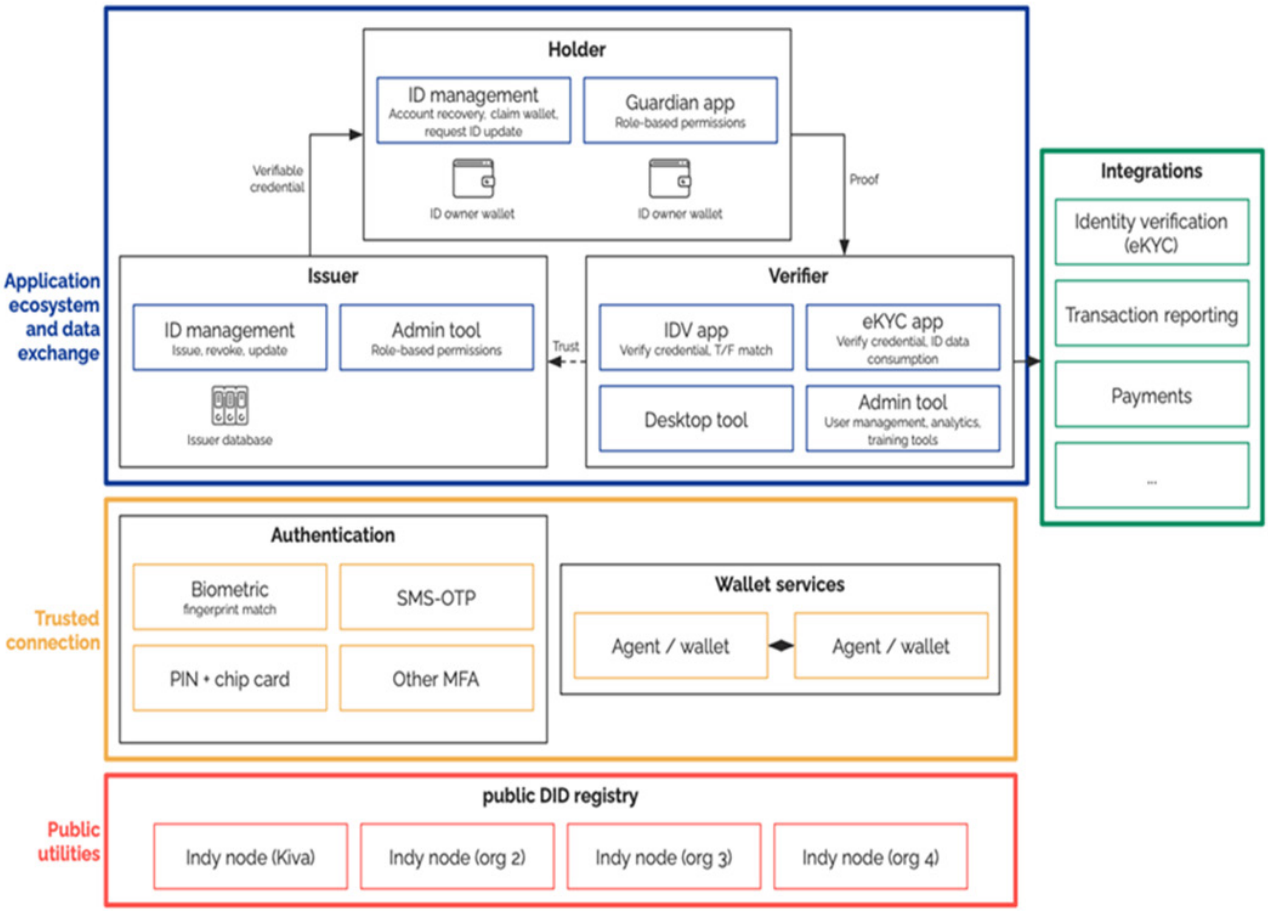
The next layer of the architecture enables trusted connections through authentication services and wallet services. For authentication, the NCRA collected biometric information as part of its identity registration efforts starting in 2018. All NCRA-issued identification credentials can be authenticated using a fingerprint bio matcher service developed and implemented in Sierra Leone. Wallet services enable citizen credentials to be stored in wallets with agent communication tools to enable peer credential exchange.

Together, these tools enable citizens to securely authenticate and access their digital wallet, and then send and receive credentials using the wallet agent-to-agent communication protocol.

5.1.3 Application ecosystem and data exchange

Using the technologies from the first two layers, citizens are provided a real-time, secure, user-centric identity verification process that can support e-KYC. In Sierra Leone, the NCRA is the issuer of over 3.6 million digital IDs, with ID management and adminis-

Figure 8: Summary architecture



trative tools integrated into its existing identity registration and management processes. These ID credentials are held in guardianship under a data protection agreement with the NCRA, which enables citizens to access and manage their data securely through a fingerprint bio matcher service. Verifiers (FSPs) are then able to request customers (or prospective customers) share their official identity credentials for e-KYC or CDD.

The NDIP is made available to FSPs through simple verifier integration APIs and whitelabel applications that FSPs can integrate directly into their existing onboarding and compliance processes.

The summary architecture is presented Figure 8.

All of this translates into seamless experience for individuals attempting to open a new account with an FSP:

a) A customer visits their local FSP office.
b) They enter their national ID number and provide their fingerprint.
c) A disclosure notification informs them of the data they will share with the FSP.
d) Upon consent, the data are shared from their wallet to the FSP.
e) The FSP uses these data to verify customer identity, fulfil KYC compliance requirements, and open the account.

5.2 Open Standards

Kiva Protocol adheres to the Principles on Identification for Sustainable Development which call for open standards and vendor neutrality in the design of digital identity systems to encourage innovation and ensure financial and operational efficiency and sustainability. Much of the foundational code used in Kiva Protocol is hosted at the Linux Foundation with-

in the open source Hyperledger Project. Especially relevant sub-projects within Hyperledger are

a) **Hyperledger Indy**: tools, libraries, and reusable components for providing digital identities rooted on blockchains so that they are interoperable across administrative domains, applications, and any other silo.
b) **Hyperledger Aries**: a shared, reusable, interoperable tool kit designed for solutions focused on creating, transmitting, and storing verifiable digital Credentials in blockchain-rooted peer-to-peer interactions.
c) **Hyperledger Ursa**: a shared cryptographic library to avoid duplicating other cryptographic work and increasing system security.
d) **Hyperledger Identity Working Group**: discussion, research, and documentation of methods to capture, store, transmit, and use identities in blockchain, specifically for projects within Hyperledger.

To maintain compatibility across independent implementations, the Hyperledger community maintains a directory of ratified message types and protocols that are generally accepted as necessary, should the software in question support the functionality. The current state of interoperability can be found in the Aries-RFC directory, and is described in the Aries Interoperability Profile RFC.

A strong advantage of this type of standardized identity protocol derives from the interoperability, efficiency, and network effects that can be achieved by working together:

a) **No vendor lock-in.** Because Kiva Protocol is open-source software, the implementing entity (typically a government agency or public-private partnership) is not reliant on a single vendor to maintain or modify the system.
b) **Standards.** Technical standards and terminology are shared across the open-source community. This greatly simplifies integrating Kiva Protocol into existing or new systems for governments, FSPs, and other authorized entities.
c) **Interoperability and Extensibility.** Enabling Kiva Protocol to extend beyond e-KYC verification is possible if desired. Adding adjacent services such as business entity registration, digital driver's licenses, digital voter identity, portable health data, and verifiable education records are just a few examples. Moreover, because Kiva Protocol extends the functionality of existing identity systems – whether national ID systems, functional IDs, or social protection eligibility lists – it can be deployed without interruption to existing public or private sector programs.
d) **Resilience.** The open-source nature of Kiva Protocol makes it resilient in that no external party can revoke the ability to use the system. In addition to removing vendor lock, even if all external access to the system were cut off, local operators would be able to provide a then-current copy of the ledger data, and clients would be able to continue with new local-only transactions until a time when updates can be merged back into the national system.

5.3 Implementation Status

With the digital wallet infrastructure in place, Kiva began supporting individual FSP API integrations into the NDIP in early 2020. When complete, this integration work will enable citizens to share verifiable credentials from their digital wallet directly into the core banking systems of FSP verifiers. Given the technical capacity constraints across the sector – particularly in Sierra Leone's remote provinces – Kiva's in-country teams worked intensively with early FSP pilot partners to ensure that the NDIP-based identity verification integrated seamlessly into existing workflows and customer onboarding processes.

6 INTRODUCTION TO ADIA FOR DID IDENTITY SYSTEMS

The Accountable Digital Identity Association (ADIA) is a technology specification from DID Alliance (DIDA). The Decentralized Identity (DID) Alliance is an open industry association created to drive the development of a standardized, interoperable framework for decentralized identity services to ensure the authenticity of and establish trust in digital identities. The group will contribute to the creation of a global ecosystem, the formation and operation of a collaborative network, the diffusion of standardized technologies and the development of the decentralized identity industry

ADIA's purpose is to achieve true interoperability among decentralized identity (DID) systems by deploying requisite technologies and processes that are outside the scope of existing interoperability efforts such as W3C, DIF, and Hyperledger Aries. In pursuit of this objective, ADIA's efforts are directed to three main areas:

- **Trust sourcing**

ADIA relies on trusted sources to bootstrap the digital identity of individuals. ADIA work is based on ITU-T Recommendation X.1254, whereby an identity vetting assurance level during the process of validating an individual before a digital address is assigned to them. Identity resolutions process are incorporated to ensure the uniqueness of the individual with domains.

- **Cross-ledger transaction support**

ADIA works with the assumption that identity information for the individual is stored in a cloud environment with the binding to a specific digital wallet and a specific ledger. ADIA uses cloud based techniques to ensure that any application can integrate with the available claims for a given individual with interoperability ensured by using standard based cloud protocols.

- **Inclusiveness**

ADIA is an open platform, there is no royalties or rules that prevent any participant from belonging and contributing to the system

The DID Alliance seeks to fulfil the promise of DID systems by helping to solve some of the most important practical problems attached to their operation and adoption by enabling a business interoperability layer as well as a technological one.

6.1 How ADIA works?

When the ADIA system is implemented, it will enable easy e-KYC for online and offline service providers by leveraging the universe of connected DID identity platforms that will interoperate and allow user identification via a *Digital Address*.

6.1.1 Digital Address Format

The plan is for a ADIA Digital Address to comply with the W3C standard format for DIDs.

For ADIA, the proposed format is:

did:adia:1234567ABCDEFGHI

This address would comply with the W3C standard and would be resolvable using the Universal Resolver project that is proposed by DIF.

It is comprised of the standard components of a DID:

a) URL scheme identifier (did)
b) Identifier (proposed) for the DID method (ADIA)
c) DID method-specific identifier (this would be proprietary to ADIA and would involve the DID Alliance's patent-pending "Identity Disambiguation" process).

6.1.2 Digital Address Issuance

There are two types of Issuers in the ADIA ecosystem: Verifiable Credentials Issuers and Digital Address Issuers. As the latter, an Issuer is capable of identity verification to meet regulatory KYC requirements. Verifiable Credential Issuers leverage the KYC capability of Digital Addresses to append other identity claims as Verifiable Credentials.

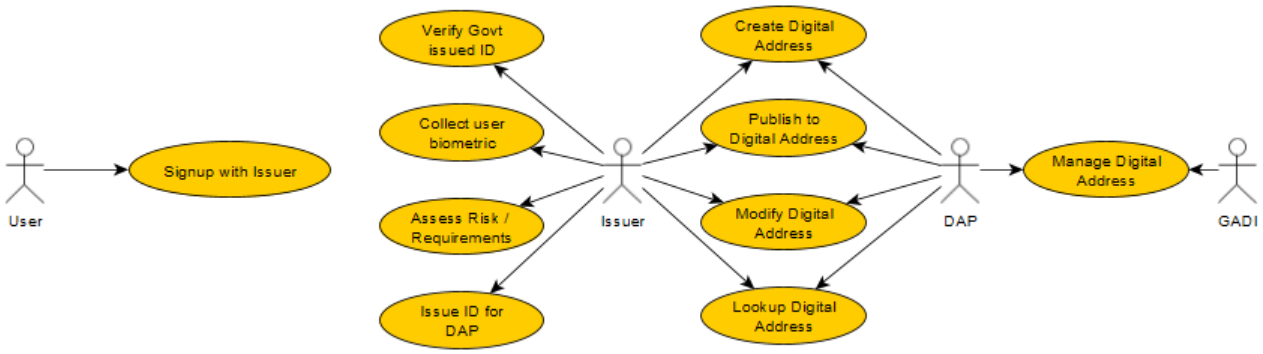
The Digital Address is a special ADIA identifier that is issued to an individual by a certified Digital Address Issuer after in-person KYC has been done. Candidates for such certification could be entities such as banks who have established in-person accounts, certain government agencies, insurers, etc. By using a specialized biometric sensor, the Issuer will combine a biometric characteristic from the individual user, combine it with certain other identity-related traits (such as first name, last name, date of birth, city of birth, etc.) and after applying a hashing algorithm, derive a Digital Address in cooperation with a participating Digital Address Provider (DAP). Digital Address Providers are solution providers who are currently providing DID-related identity services. The Digital Address may be delivered to a FIDO-secured Credential Wallet on the user's smartphone (or other embodiments) as well as could be presented as a card secured by a user-defined PIN. In both cases, the Digital Address is strongly bound to the individual user by the combination of identity attributes and biometric measurement taken from that user.

The Digital Address Issuer has access to a limited number of APIs (Create Digital Address, Publish to Digital Address, and Update Digital Address – which can be used for credential revocation when necessary.)

6.1.3 ADIA layered model

The ADIA layered model focus on separating the identity-based services at the business layer from the network security and data layer (See Figure 10). The objective here is to have a trusted identity layer that enable business logic while protected by a data security layer.

Figure 9: Issuing Digital Address to User



6.2 Use of QR codes in ADIA

QR codes are integral for modern authentication flows and that is no exception for the Digital Address. A technical committee (TC) has been established in OASIS, which addresses some of the problems of QR-based authentication flows and guidelines for enhanced QR security will be created. The OASIS TC will survey QR based methods that online relying partners and service providers currently use to authenticate electronic identities. The TC will compare these methods to propose a set of protocols service providers can reliably use. The set of protocols will enable authentication without static credentials or passwords, and provide increasing levels of identity assurance, risk mitigation, and authentication certainty.

6.3 User flows for e-KYC

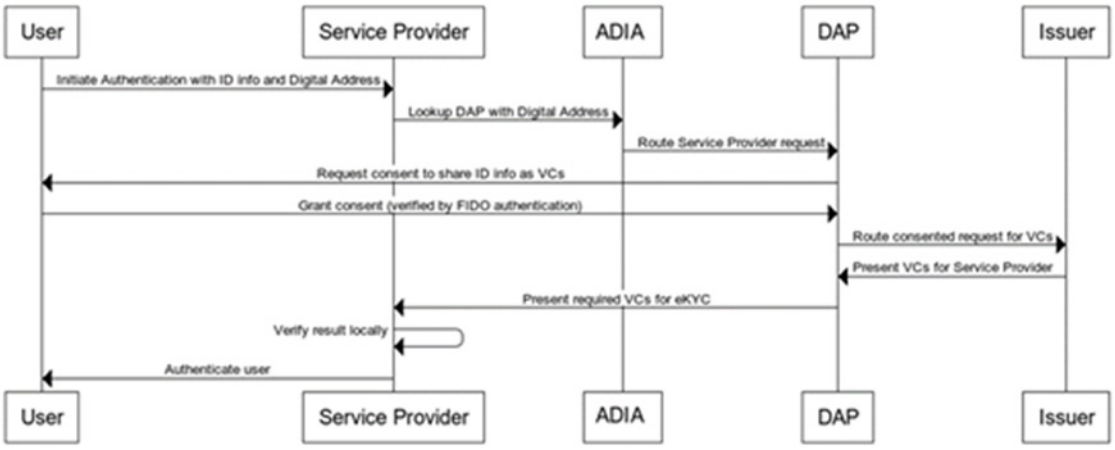
6.3.1 In-person e-KYC

A user wishing to identify themselves in an in-person interaction will supply the identity attributes required to meet the requirements set up by the Service Provider (for example an individual wishing to open a new bank account at a local branch).

In addition to their name, address, place of employment, etc., the user will supply their Digital Address. The Service Provider can check the identity attributes of the user along with the Digital Address via a ADIA web interface. When the Service Provider inputs the user data along with the Digital Address, the request for a DID-based verifiable credential (with the same identity data fields requested) will be

Figure 10: ADIA layer model

Figure 11: User e-KYC using ADIA to lookup DAP-managed Verifiable Credentials



routed to the Digital Address Provider that provides the user's Credential wallet. The user will receive a notification via their smart device asking for their consent to provide the identity attributes required by the Service Provider. When the user grants consent and verifies themselves locally on their device using FIDO authentication, the successful verification will trigger the DAP process to route the Issued VCs back to the Service Provider.

6.3.2 Remote e-KYC (online sign-up for website or app)

The system works the same but instead of the user presenting identity data in person for a Service Provider to input into their terminal, the user self-inputs identity data to be verified along with their Digital Address.

The level of assurance of the identity of the user is the same remotely as it is in person since the assurance of the original Digital Address is secured with a FIDO registration at the time of Issue.

6.4 ADIA wallet interoperability

As mentioned above, there are numerous ledger-based DID-focused identity platform initiatives underway. What separates the ADIA project of DID Alliance is a focus on true ledger interoperability. By leveraging existing communications protocols (like the Hyperledger Aries project and DIDCOM by the DIF for identity flows along with a smart contract layer for business flows) ADIA will extend those protocols to truly operate among disparate ledger systems, rather than different instances of the same ledger technology. This coupling of cross-ledger communication with a way to settle cross-ledger payments via 3rd party market makers (which can provide liquidity among token types) enables a truly agnostic inter-ledger ecosystem where the whole is greater than the sum of the member parts.

By not relying on device-based credentials, certain other challenges (e.g., multiple device support) are also alleviated. Wallets may be designed to control cloud-based credential metadata which is created from actual issuer data and controlled by the user via interactions with strong authentication (e.g., FIDO).

6.4.1 ADIA interoperability with FIDO

ADIA uses FIDO authentication at the application layer to ensure that the task of accessing verifiable credentials is protected through secure authentication. Any FIDO protocol can be used to secure the access to the ADIA application wallet. Interoperability is ensured at the authentication layer by ensuring the usage of FIDO certified products.

6.4.2 QR code security

QR code passwordless authentication methods are vulnerable to man in the middle attacks. In OASIS there is a working that is focused on securing the usage of QR code in passwordless authentication methods.

6.5 Standardization

The standardization work of the DID Alliance is not focused on developing new protocols, but rather standardizing the interoperability of existing protocols. Additionally, it will focus on publishing common schema for identity and credentials used within

specific industries (e.g., healthcare, financial services, etc.)

With ADIA in service and employing a global standard, the various DID-implementing identity solutions will no longer have to be siloed ecosystems. Any Issuer or Service Provider wishing to leverage DID-based authentication or customer on-boarding will also no longer have to "pick a winner" in the space – hoping that they have chosen to integrate with the one "winning" stack. For Issuers, they will be able to trust that the credentials they issue will reach a potentially global audience of Service Providers and likewise, Service Providers will be able to consume any type of ADIA-certified Verifiable Credential. With the associated personal identity data (PID) remaining safely with the original identity Issuer, organizations within countries with strict data export controls are still able to participate, since no PID crosses borders.

Alongside the technology, there are standards necessary for establishing "identity roles" or "what we do." With this system it is possible to create and use portable credentials that truly establish the holder as a student or doctor (for example) – by leveraging industry bodies that can provide definitions of what constitutes legitimate and credential-able bona fides to use such a title. Similarly, credentials which may be used for financial transactions can be established which meet global AML/CFT standards.

7 PROPOSED REQUIREMENTS FOR A STANDARD FOR DECENTRALIZED ID FOR E-KYC

The COVID-19 pandemic has accelerated the pace towards digitalization of government payments, from e-commerce to e-banking, remote onboarding for digital finance, everything is getting transformed digitally to make it easier and more convenient for users. However, with major security threats like transaction fraud, identity theft, and other cyberattacks compromising personal data of customers; it becomes essential that actions are taken to protect customer data and privacy in the digital interactions. To counter these challenges, blockchain-based emerging solutions like Decentralized Identity and Verifiable Credentials has the potential to disrupt the identity and verification domain by protecting data privacy, sharing data with user-consent and securing transactions, while enhancing the overall e-KYC process and user experience.

Decentralized ID is a type of user-centric identity that is created, owned, and managed by users of their free will (it is sometimes referred to as self-sovereign identity). The user is identified with a Decentralized Identifier (DID) which is globally unique. Each DID has associated cryptographic material that helps in authenticating users and verifying credentials that are issued to or presented by them. A verifiable credential allows the user to digitally issue credentials and sign it cryptographically, which can be verified with the help of the distributed ledger or blockchain. This ensures various credentials like educational qualification, job history, personal details, licenses, certificates, etc., are accessible to the authorized parties in a tamper-proof and authenticated manner.

A distributed ledger or a blockchain forms the backbone of a decentralized identity system. User DIDs can be private or public. Decentralized identity use for e-KYC will be strengthened for use if the users acquire the credentials digitally the government organization as issuer. The credentials are acquired and stored digitally in an identity wallet. They can also be presented to financial services organizations where the verifications can be done digitally thus enabling remote onboarding and identity verification. This section considers requirements for a standard for decentralized identifiers using distributed ledgers and verifiable credentials for e-KYC for digital finance. The standard will address the following areas:

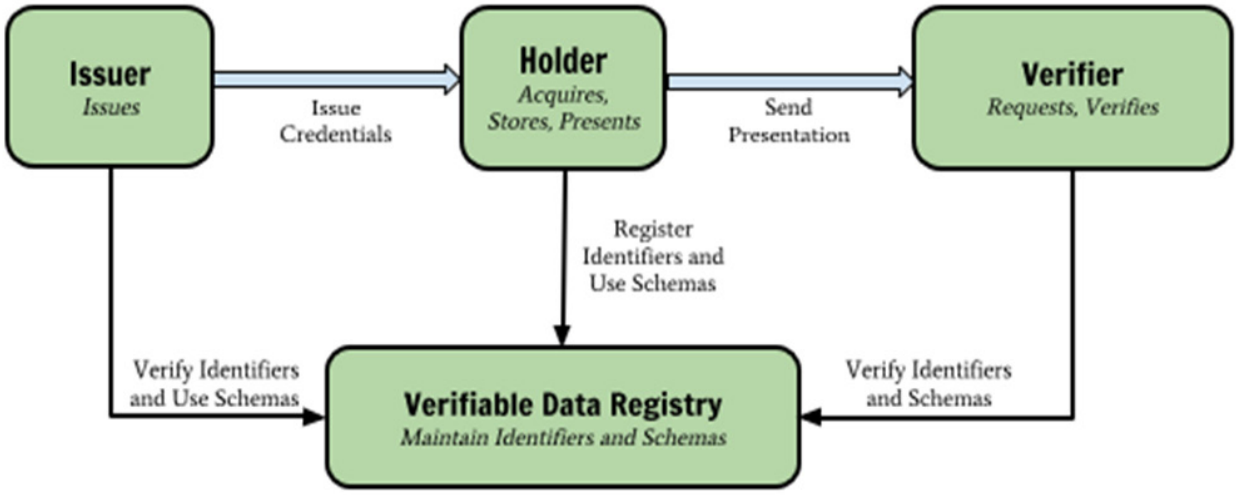
- Creation of the decentralized identifier and anchoring to be able to perform identity-related activities such as e-KYC;
- Issuance of the verifiable credential by the Issuer, delivery of the verifiable credential and the recording of the information related to the issuance of such Credential on the distributed ledger; and
- the Presentation process which is the most common action required by Verifiers to verify the user identity (e.g., e-KYC) before providing the service.

7.1 Stakeholders roles and information exchange

Figure 12 shows the main roles of stakeholders involved and the information flow.

The main roles for the stakeholders and information flows above are described below:

Figure 12: Roles and Relationships of Verifiable Credentials



Issuer
A role an entity might perform by asserting claims about one or more subjects, creating a verifiable credential from these claims, and transmitting the verifiable credential to a holder. In the context of digital finance, this would be a government entity or any such entity having this mandate, in terms of issuing an identity credential based on the national identity of the holder. These verifiable credentials are held by citizen-controlled and -permissioned digital wallets.

Verifier
A role an entity might perform by receiving one or more verifiable presentations for processing. Other specifications might refer to this concept as a relying party. In digital finance, the Verifier will be the party who will perform the e-KYC verification (e.g., the DFS provider).

Holder
A role an entity can perform by possessing one or more verifiable credentials. A holder is usually, but not always, the subject of the verifiable credentials they are holding. Holders store their credentials in credential repositories. Any Holder with an identity credential issued by the government will be able to securely authenticate their official identity with digital financial services providers to support e-KYC for new account opening and ongoing customer due diligence (CDD).

Verifiable data registry
A role a system might perform by mediating the creation and verification of identifiers, keys, and other relevant data, such as verifiable credential schemas and revocation registries, which might be required to use verifiable credentials. In the context of e-KYC for digital financial services, this would be a network of nodes supporting a public decentralized identity (DID) registry. This registry provides the foundation of trust in the digital credentials used to verify identity.

Verifiable Credentials
From the W3C Verifiable Credentials Data Model specification:

A verifiable credential can represent all the same information that a physical credential represents. The addition of technologies such as digital signatures makes verifiable credentials more tamper-evident and therefore more trustworthy than their physical counterparts.

A Verifiable Credential request can be made by sending a specific message from the Holder to the Issuer (using off-chain communication mechanism). The identity information is embedded in the verifiable credential delivered through a secure off-chain channel by the Issuer to the Holder. This information is never sent through, nor stored on the distributed ledger. There is a proofing mechanism (e.g., a signature) embedded within the verifiable credential.

Presentations

Holders/Users can generate presentations and share them with verifiers to prove they possess verifiable credentials with certain characteristics. Both credentials and presentations can be rapidly transmitted, making them more convenient than their physical counterparts when establishing trust at a distance.

When a Holder wants to access a digital finance service, the Verifier could need some information about the Holder, prior to accept providing the service. The specific required information is requested using a presentation request, specifying the purpose and the minimum required information with respect to that service.

The Holder then sends a verifiable reply with the appropriate Credentials from the ones stored in their wallet (not the distributed ledger). The Holder may need to register information related to the presentation process on a distributed ledger. Another information of the reception may be registered independently by the Verifier in the same distributed ledger.

7.2 Verifiable credential requirements

The following requirements are proposed for Verifiable Credentials (request, issue, delivery, and receipt):

a) The content should conform to W3C recommendation "Verifiable Credentials Data Model 1.0".
b) The verifiable credentials should support existent and future attribute naming schemas such as X.520, schema.org, ISO 20022 or industry specific standards.
c) The verifiable credential would include the following information:

- General information about the purpose for use;
- Verifiable Credential identifier;
- Holder information, including the list of Holder's attributes, as per request, and the Holder's DID;
- The Issuer information, including the Issuer's DID;
- Date verifiable credential was issued;
- Metadata about the digital identity management system used which could be for instance the level of assurance of the Holder attributes;
- Issuer's digital signature; and
- Expiry date of Verifiable Credential if applicable.

d) Verifiable credential request by Holder/User

- The Holder should make the request to an Issuer using a secure off-chain channel with mutual DID proof of possession.

e) Issuance to Holder.

- Issuers should create Credentials only as a response to a request from the Holder.
- All the information defined in W3C recommendation "Verifiable Credentials Data Model 1.0"
- should be complied with by the Issuer.
- After being created, the verifiable credential, should be sent to the Holder using a
- secure off-chain channel with mutual DID proof of possession.
- Verifiable credentials shall not be shared directly to any other entities by the Issuer.
- The issuance event must be registered on the distributed ledger, by the Issuer.
- The delivery event must be registered on the distributed ledger, by the Issuer.
- The verifiable credential shall not be directly recorded on the distributed ledger.

f) Receipt of verifiable credential

- Verifiable credential digital signature shall be validated upon reception.
- The Verifiable credential may be accepted, or not, by the Holder/User.
- The Verifiable credential shall be stored in a digital wallet under the sole control of the Holder, in the original format without any modification to the content.
- The receipt of the verifiable credential may be registered on the distributed ledger, upon acceptance, by the Holder.

7.3 Decentralized Identifier (DID)

The Decentralized Identifier (DID) specifications are being created to establish a cryptographically verifiable, globally addressable identifier namespace for distributed ledger and blockchain systems. Decentralized Identifiers are the addressing scheme used for Verifiable Credentials.

The DID design goals should include the following principles:

a) Decentralization: DID architecture should eliminate the requirement for centralized authorities or single points of failure in identity management, including the registration of globally unique identifiers, public verification keys, service endpoints, and other metadata.
b) Entity control of identifiers: DID architecture should give entities, both human and non-human, the power to directly control their own digital identifiers without the need to rely on external authorities.
c) Personal Identifiable Information Protection: DID architecture should enable entities to control the identifiable data of their digital identities, including minimal, selective, and progressive disclosure of attributes or other identity data.
d) Security: DID architecture should enable sufficient security for relying parties to depend on DID records for their required level of assurance.
e) Proof-based: DID architecture should enable an entity to provide cryptographic proof of authentication and proof of authorization rights.
f) Discoverability: DID architecture should make it possible for entities to discover DIDs for other entities to learn more about or interact with those entities.
g) Interoperability: DID architecture should use interoperable standards so DID infrastructure can make use of existing tools and software libraries designed for interoperability.
h) Portability: DID architecture should be system and network-independent and enable entities to use their digital identities with any system that supports DIDs and DID Methods.
i) Simplicity: To meet these design goals, DID architecture should be "as simple as possible but no simpler".
j) Extensibility: When possible, DID architecture should enable extensibility provided it does not greatly hinder interoperability, portability, or simplicity.

From the W3C Decentralized Identifier draft specification:

a) The emergence of distributed ledger technology (DLT), sometimes referred to as blockchain technology, provides the opportunity for fully decentralized identity management. In a decentralized identity system, entities are free to use any shared root of trust. Globally distributed ledgers (or a decentralized P2P network that provides similar capabilities) provide a means for managing a root of trust with neither centralized authority nor a single point of failure. In combination, DLTs and decentralized identity systems enable any entity to create and manage their own identifiers on any number of distributed, independent roots of trust.
b) The entities are identified by decentralized identifiers (DIDs). They may authenticate via proofs (e.g., digital signatures, privacy-preserving biometric protocols, etc.). DIDs point to DID Documents. A DID Document contains a set of service endpoints for interacting with the entity. Following the dictums of Privacy by Design, each entity may have as many DIDs as necessary, to respect the entity's desired separation of identities, personas, and contexts.
c) To use a DID with a particular distributed ledger or network requires defining a DID method in a separate DID method specification. A DID method specifies the set of rules for how a DID is registered, resolved, updated, and revoked on that specific ledger or network.
d) This design eliminates dependence on centralized registries for identifiers as well as centralized certificate authorities for key management—the standard pattern in hierarchical PKI (public key infrastructure). Because DIDs reside on a distributed ledger, each entity may serve as its own root authority – an architecture referred to as DPKI (decentralized PKI).

7.4 DID Requirements and Authentication

Some requirements proposed for DIDs are as follows:

a) Entities must be able to self-manage their own DIDs on a distributed ledger, using a DID method.
b) The DID method must conform to W3C working draft "Decentralized Identifiers (DIDs) v1.0".
c) the DID method must ensure the Holder/User is the exclusive DID owner, (e.g., the private key corresponding to the public key used to authenticate the DID controller).
d) when assisted by a third party in the DID creation process, any party must always maintain the DID's sole control.
e) A DID shall be anchored on a distributed ledger.
f) A DID must be universally resolvable to its corresponding DID document.
g) The DID document may be produced upon demand when dereferencing the DID; and
h) A DID document for a natural person must not be stored in a distributed ledger, except for its

public key which could be on the distributed ledger.

DID Authentication enable a DID Holder to prove control over a DID during its interaction with a Verifier (sometimes referred to as Relying Party). DID authentication should support web and mobile flows.

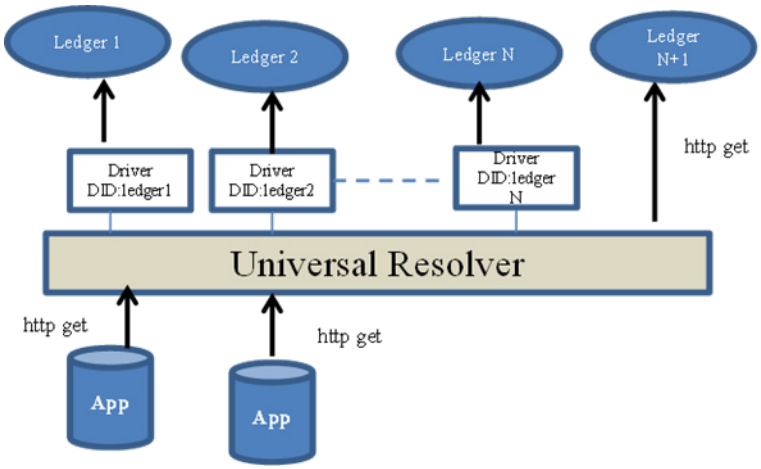
The following general steps to be executed by the Verifier include:

a) The Verifier retrieves the DID Document associated with the DID Holder.
b) The Verifier uses the authentication property of the DID Document to determine how to perform DID authentication, for example cryptographic signatures, proving control of a public key or use of an authentication service endpoint.
c) The Verifier executes the authentication mechanism provided.

7.5 DID Resolution

The DID specification requires each DLT to have a DID Method specification to describe how DID operations are performed. The implication of having many DID Method specifications is that resolving a text string, the DID, to locate the trust root and the associated DID Document is complex. The DID resolution function could become a major impediment to interoperable DIDs. Work has begun on a universal DID resolver architecture and toolset that can take any valid DID as input and resolve it to a DID Document. The universal resolvers are specifically designed to work for decentralized identifiers and support DID resolution over many different types of DLT. The universal resolver approach solves the problem of heterogeneous networks having different method specifications for their own DID. Figure 13 depicts the Universal Resolver concept.

Figure 13: Universal DID Resolver



7.6 Decentralized Identity Wallets

The individual must have software and/or hardware that enables them to interact with the decentralized identity system. These components are agents and wallets.

The primary function of an agent is to communicate with other agents and coordinate DID resolution and authentication. The agent keeps track of DIDs related to other entities in the network. An agent contains or is connected to a wallet where cryptographic secret keys are kept and protected. The wallet contains the essential private keys that allow the individual to prove control over a DID and thus participate in the decentralized identity system. The agent and wallet hold verifiable credentials and proofs belonging to the individual.

The wallet can be entirely on the user's device or a virtual wallet where one part of the wallet is on the user mobile device and another part in the cloud. The latter configuration enables the creation of agents to act on behalf of the user and perform services without the need for user direct involvement.

8 REFERENCES

[1] https://www.itu.int/en/ITU-T/extcoop/figisymposium/Documents/ITU_SIT_WG_Implementation%20of%20Secure%20Authentication%20Technologies%20for%20DFS.pdf.

[2] https://fidoalliance.org/

[3] http://didalliance.org/content.php.

[4] https://www.w3.org/TR/vc-data-model/#dfn-verifiable-credentials.

[5] http://www.fatf-gafi.org/media/fatf/documents/recommendations/pdfs/Guidance-on-Digital-Identity.pdf

[6] http://www.sbp.org.pk/bprd/2016/C9.htm.

[7] https://www.w3.org/TR/vc-data-model/.

[8] http://documents1.worldbank.org/curated/en/213581486378184357/pdf/Principles-on-identification-for-sustainable-development-toward-the-digital-age.pdf.

[9] https://www.linuxfoundation.org/.

[10] https://www.hyperledger.org/.

[11] https://www.hyperledger.org/use/hyperledger-indy.

[12] https://www.hyperledger.org/use/aries.

[13] https://www.hyperledger.org/use/ursa.

[14] https://wiki.hyperledger.org/display/IWG.

[15] https://github.com/hyperledger/aries-rfcs/blob/master/index.md.

[16] https://www.w3.org/TR/did-core/#a-simple-example.

[17] https://iiw.idcommons.net/DIF_%E2%80%93_Universal_Resolver_+_Universal_Registrar_(DID%E2%80%99s_across_blockchains

[18] https://www.w3.org/TR/did-core/#dfn-did-methods

[19] https://www.oasis-open.org/committees/tc_home.php?wg_abbrev=esat

[20] https://identity.foundation/working-groups/did-comm.html

[21] D. Reed, M. Sporny, D. Longley, C. Allen, R. Grant and M. Sabadello, "Decentralized Identifiers (DIDs) v0.11," 23 August 2018. https://w3c-ccg.github.io/did-spec/.

[22] M. Sabadello, K. Den Hartog, C. Lundkvist, C. Franz, A. Elias, A. Hughes, J. Jordan and D. Zagidulin, "Introduction to DID Auth," 26 07 2018. Available: https://github.com/Weboftrustinfo/rebooting-the-web-of-trust-spring2018/blob/master/final-documents/did-auth.pdf.

[23] M. Sabadello, "A Universal Resolver for self-sovereign identifiers," 01 11 2017. https://medium.com/decentralized-identity/a-universal-resolver-for-self-sovereign-identifiers-48e6b4a5cc3c.

[24] D. Reed, J. Law, D. Hardman and M. Lodder, "DKMS (Decentralized Key Management System) Design and Architecture," 02 04 2018. https://github.com/hyperledger/indy-sdk/blob/677a0439487a1b7ce64c2e62671ed3e0079cc11f/doc/design/005-dkms/DKMS%20Design%20and%20Architecture%20V3.md.

International Telecommunication Union
Place des Nations
CH-1211 Geneva 20
Switzerland