eKYC Interoperability Standard Proposal

Version: 1.1

Oct-17-2023

Prepared By

TUM SEREY VATHANA

Techo Startup Center

eKYC Interoperability Standard Proposal

REVISION: 1.1 REVISION DATE: 17-Oct-2023

PREPARED BY: TUM SEREY VATHANA

Table of Contents

1. Introduction

The Open KYC verification API offers a range of valuable features and functionalities for eKYC providers. Within the service, eKYC providers can leverage APIs to verify client information with the data from the General Department of Identification, validate face similarity, conduct video liveness verification, and perform OCR on identification documents such as national ID cards or passports, among others. As of the publication date of this document, a total of 2.5 million API requests have been made by banks, microfinance institutions, and insurance companies. This collection of APIs plays a crucial role in ensuring the accuracy of user information and biometric data, enabling these companies to offer reliable services to the people of Cambodia.

However, a significant limitation is that the eKYC information remains confined within the domain, services, and applications of the respective provider. Consequently, the potential for sharing and collaborating on eKYC information among institutions or SMEs is restricted. This lack of data interoperability hampers the seamless exchange of eKYC data and inhibits opportunities for cooperation and information sharing. To fully realize the benefits of eKYC, it is crucial to address this limitation and establish mechanisms that facilitate secure and efficient sharing of eKYC information among different entities, enabling collaboration and enhancing the overall effectiveness of customer verification processes.

The eKYC Interoperability Standard outlined in this document enables secure collaboration and data exchange among key stakeholders while preserving user privacy. It establishes protocols, formats, and security measures to ensure the seamless exchange of eKYC information while maintaining data security and privacy protection.

2. Conventional eKYC vs eKYC Interoperability Standard

2.1. Conventional eKYC

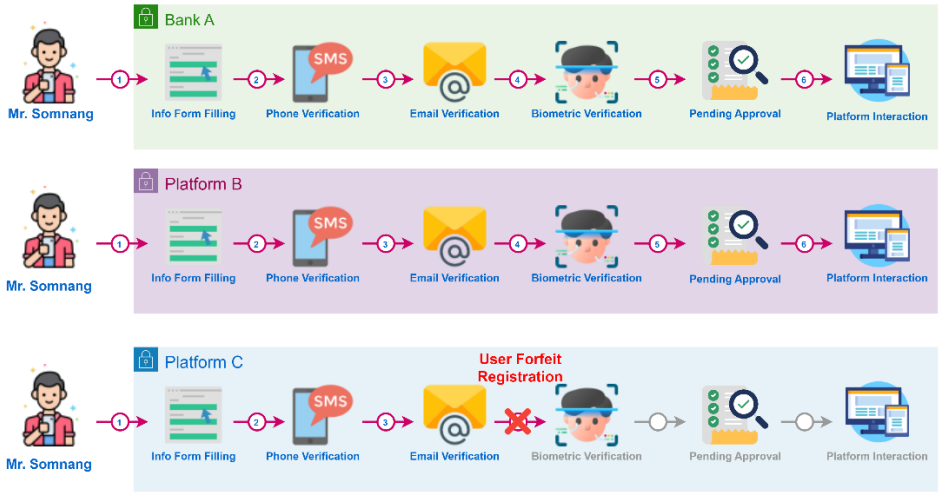

Figure 1 User's experience using conventional eKYC

In the conventional eKYC process, individuals like Mr. Somnang face several hurdles when registering on digital platforms. He is required to input personal information, undergo mobile, email or document verification, provide facial data, and wait for approval from each platform. This repetitive registration process becomes burdensome and discourages participation in digital services. Moreover, eKYC providers bear significant costs associated with verifying user input, including information, phone, email, document and biometric verification. The complex registration procedure increases user frustration, ultimately leading to the abandonment of registration and the loss of potential users.

2.2. eKYC Interoperability Standard

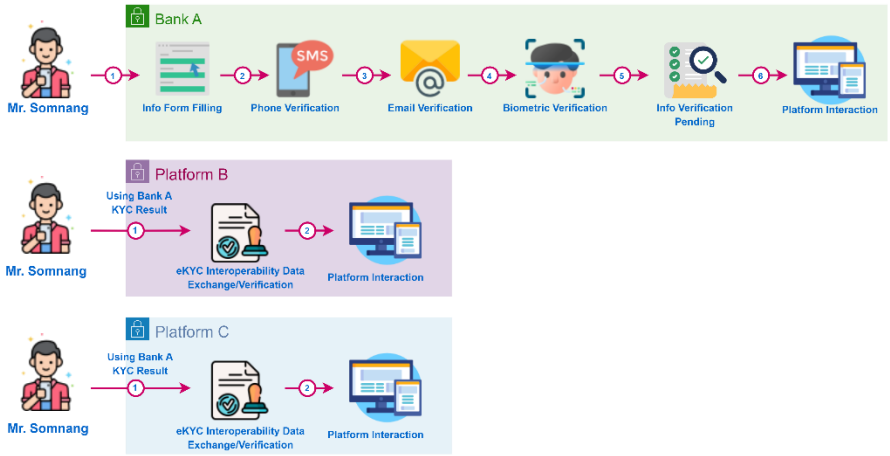

Figure 2 User's experience using eKYC Interoperability Standard

The eKYC Interoperability Standard offers a significant improvement in user experience and cost reduction for customer eKYC processes. With this standard, Mr. Somnang only needs to perform a full eKYC process with a single platform. Subsequently, when he wishes to register or authenticate himself with another platform, he can effortlessly reuse the eKYC result from the previous platform, eliminating the need for manual input of information, submission of official documents, or biometric data. This standard is designed to enhance user convenience by enabling the reuse of eKYC results across multiple platforms, extending the scope of the one-only principle beyond e-government. It promotes collaboration among eKYC providers and platforms that require eKYC, allowing them to take full advantage of this standardized approach.

3. Problem Statements

3.1. Private, Public Institution

3.1.1. Regulatory Compliance

Complying with eKYC (electronic Know Your Customer) regulations necessitates the implementation of robust processes that require substantial investments in technology, infrastructure, and personnel. Private institutions must allocate significant resources to

develop or acquire sophisticated identity verification systems capable of securely and accurately verifying customer information in real-time. This involves integrating various data sources, leveraging advanced analytics techniques, and incorporating artificial intelligence (AI) technologies to enhance the reliability and effectiveness of the eKYC process.

To begin with, implementing robust eKYC processes requires investment in technology. Institutions need to develop or adopt specialized software and systems that can handle the complexities of identity verification. These systems should be capable of securely handling sensitive customer data, performing identity checks against multiple reliable data sources, and ensuring compliance with data protection regulations. Building such technology infrastructure often involves significant upfront costs in terms of software development, hardware acquisition, and cybersecurity measures.

3.1.1. Investment & Operational Cost

The integration of the Open KYC Verification API through CamDX (Cambodia Data Exchange) brings significant advantages to eKYC (electronic Know Your Customer) providers. By leveraging this API, these providers can verify customer information using a trustworthy source, ensuring accuracy and reliability. Additionally, the integration grants them access to advanced OCR (Optical Character Recognition) capabilities within the collection of APIs provided. This OCR functionality enhances the efficiency and accuracy of data extraction from various identification documents.

However, it is important to note that such integration comes with certain financial considerations. The implementation of the Open KYC Verification API and its associated functionalities requires a amount capital investment in system development. This includes the development or modification of existing systems to integrate with CamDX and incorporate the API's functionalities. Moreover, there are ongoing operational costs associated with maintaining and supporting the integrated system.

In terms of cost recovery, eKYC registration fees heavily rely on user interaction within the platform or the services provided by the institution. This means that eKYC providers must ensure that their platform or services attract a sufficient number of users who will engage in the registration process and pay the associated fees. The success of cost recovery is directly linked to the adoption and usage of the eKYC platform, emphasizing the importance of user engagement and market demand.

The cost implications associated with the integration of eKYC (electronic Know Your Customer) systems, as discussed in the previous paragraph, can significantly limit the adoption of eKYC for small and medium enterprises (SMEs). Unlike larger institutions, SMEs often lack the necessary capital and revenue to sustain the operations required for implementing and maintaining eKYC systems. The financial burden of system development, operational costs, and ongoing maintenance can be particularly challenging for SMEs with limited resources.

Furthermore, SMEs typically do not benefit from the economies of scale that larger institutions enjoy. The larger the organization, the more customers they can distribute the costs among, resulting in a lower cost per customer for eKYC registration. In contrast, SMEs

have a smaller customer base, which means that the costs associated with eKYC registration are spread over fewer customers, resulting in a higher cost per customer. This further exacerbates the financial burden for SMEs and makes the adoption of eKYC more challenging.

As a result, many SMEs are left with no choice but to rely on traditional approaches to customer verification, which often involve trusting the user input without the means of verification. This approach carries inherent risks, as it can be susceptible to fraudulent activities and inaccurate information. However, due to the cost barriers associated with implementing eKYC, SMEs may not have access to the necessary resources or technological capabilities to implement robust verification processes.

3.1.2. Tightly Coupled Systems

APIs (Application Programming Interfaces) play a crucial role in enabling integration between systems and applications. However, APIs can have both positive and negative consequences. On the positive side, APIs provide a standardized and structured way for different components to communicate and interact, facilitating data exchange and functionality sharing. They can streamline the integration process and improve efficiency by allowing organizations to leverage existing systems and services.

However, in a tightly coupled integration, APIs can also contribute to the complexity and interdependencies between components. Changes or disruptions in one API can have a cascading effect on other components relying on it, leading to a higher risk of system failures and difficulties in making independent updates. The tightly coupled nature of the integration can create challenges in terms of versioning, compatibility, and managing dependencies. Therefore, while APIs are essential for integration, careful consideration and planning are necessary to strike a balance between the benefits and potential drawbacks of tightly coupled integration.

3.1.3. Standard and Interoperability

The lack of standardization is causing significant issues regarding interoperability among eKYC (electronic Know Your Customer) providers. Without a common set of guidelines or protocols, different eKYC systems often struggle to communicate and exchange information effectively. This lack of standardization hampers the seamless integration and interoperability of various eKYC solutions, leading to inefficiencies and complications in identity verification processes. As a result, businesses and organizations face challenges in streamlining customer onboarding, regulatory compliance, and ensuring secure and reliable identity verification across different platforms and service providers. The establishment of industry-wide standards is crucial to address these interoperability issues and enable smoother collaboration and data exchange among eKYC providers.

3.2. End-user

3.2.1. User Experience

User experience with online registration that involves complicated eKYC requirements can be frustrating and time-consuming. When users encounter an intricate eKYC process, it often involves multiple steps and the submission of various documents and personal information. This complexity can lead to confusion and difficulty in completing the registration process smoothly. Users may find themselves navigating through a labyrinth of forms and requirements, which can be overwhelming, especially for those who are less technologically savvy or unfamiliar with the eKYC process.

Complicated eKYC requirements can also result in a lengthy and tedious registration experience. Users may have to repeatedly provide the same information across different sections or platforms, which can be redundant and inefficient. The need to upload and validate numerous documents, such as identification cards, or face images can further prolong the registration process. This can be particularly frustrating for users who expect a quick and seamless experience when signing up for an online service or platform.

3.2.2. Data Privacy

Sharing sensitive personal information online during complex eKYC processes can intensify user anxiety due to inherent security concerns. Users may feel hesitant to disclose their confidential data or harbor doubts about the effectiveness of security measures implemented by the eKYC service provider. These concerns can significantly impact the user experience, leading to a sense of unease and apprehension throughout the registration process. Users may worry about the potential misuse or unauthorized access to their personal information, increasing their reluctance to participate fully in the eKYC process.

4. eKYC Interoperability Standard

The eKYC interoperability standard is designed to establish a standardized process for eKYC exchanges, encompassing information verification and attestation, secure data exchanges, consent from data owners, data formatting, and more. This standard aims to enable eKYC providers to collaborate effectively, ensuring secure and reliable exchanges while offering additional revenue opportunities. By implementing this standard, providers can offer Cambodian citizens a seamless digital registration and authentication experience, thereby fostering greater digital adoption among the population. This standardization enhances convenience and efficiency, streamlining the overall eKYC process and promoting a more accessible and user-friendly digital ecosystem in Cambodia.

4.1. Overview

In this eKYC Interoperability Standard will cover various aspect including:

- Attesting/verification mechanism: The standard leverages blockchain technology to enhance security and transparency in the verification process.
- Data exchanges for registration and authentication: Guidelines are established for secure and efficient data exchange protocols, eliminating redundant data collection.

- User privacy and consent mechanism: The standard emphasizes the protection of user privacy and compliance with data protection regulations.
- API economy of providers and requesters: Standardized APIs are defined to facilitate seamless integration and data exchange between eKYC platforms.
- Tiered eKYC and data templates: The standard defines different levels of authentication and verification based on transaction risk profiles, ensuring scalability and appropriate security measures.
- Improved user experience: Guidelines for user-friendly interfaces and simplified processes enhance the overall user experience.
- Detailing data exchanging mechanism: Protocols and formats for data exchange are established to ensure compatibility and efficiency across platforms.

4.2. Attestation & Verification mechanism

In order for eKYC results to be usable across various institutions, the eKYC data must go through an attestation process. This involves the organization that performs the eKYC verifying and validating the data to attest the result, and the requester institution being able to verify the authenticity and integrity of the data. It is crucial that the data remains tamper-proof to ensure its reliability and trustworthiness.

In the realm of multi-organization collaboration, the significance of tamper-proof and verifiable attestation cannot be overstated. For requester organizations, these attestation mechanisms play a critical role in establishing trust and reliance on the provided data. By ensuring the integrity and authenticity of attested information, requester organizations can confidently offer their services to the public. The ability to verify the validity of attestation instills a sense of confidence and reassurance, as it demonstrates that the information has not been tampered with or altered in any way. This level of trust is essential in facilitating seamless collaborations among multiple organizations, enabling them to leverage and build upon each other's verified data, ultimately leading to more efficient and reliable services for the public.

To achieve these objectives, the Open Attestation Framework and the CamDL blockchain network have been chosen for the design. The Open Attestation Framework provides a standardized approach to attestations, ensuring that the eKYC data is properly verified and validated against forgery and tempering. CamDL blockchain network is utilized to further enhance the security and integrity of the eKYC data. Blockchain technology, known for its decentralized and immutable nature, ensures that the data remains secure and tamper-proof. The use of blockchain allows for transparent and auditable records of the attestation process, providing assurance to all parties involved.

4.2.1. Open Attestation Framework

Open Attestation is an open-sourced framework to endorse and verify documents using the blockchain developed by GovTech Singapore (https://www.openattestation.com). Documents issued with framework are cryptographically trustworthy and can be verified independently.

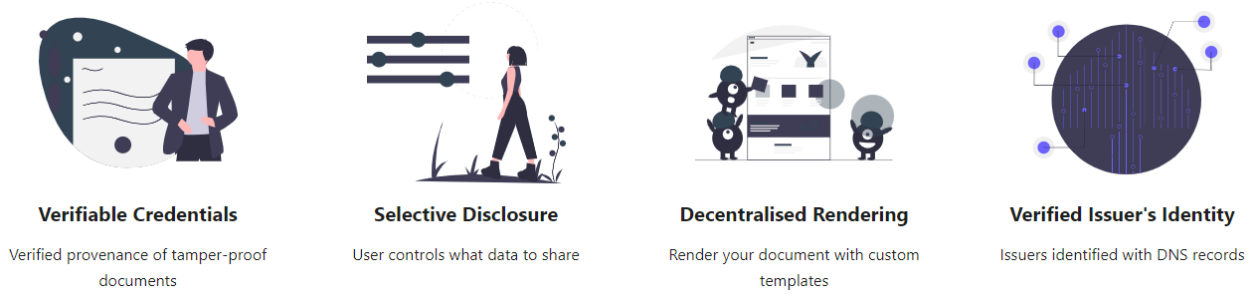

Figure 3 Principles of Open Attestation

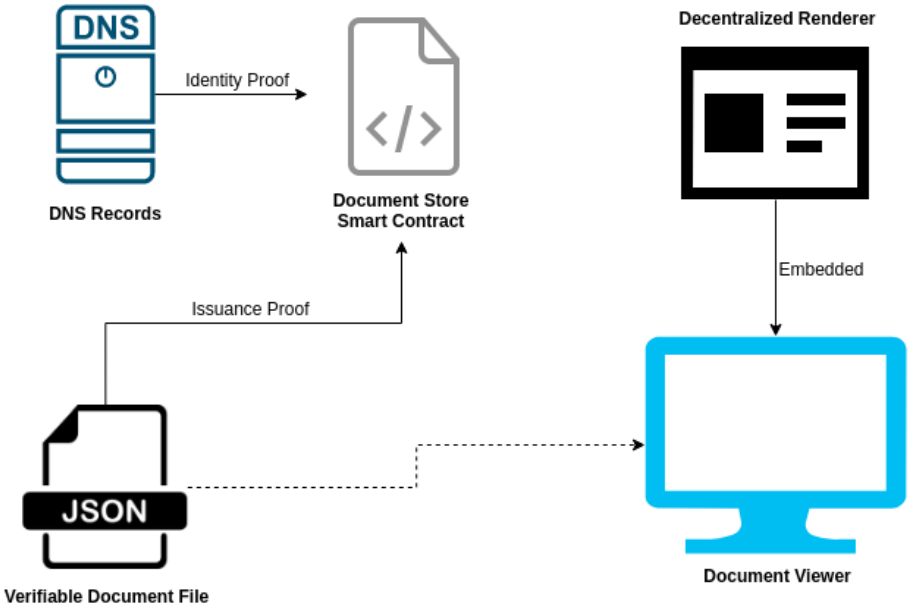

Figure 4 Overview of component in Open Attestation

- Verifiable Document: Verifiable Document (or verifiable credential) is a tamper-evident document that cryptographically proves who issued it. They are the electronic equivalent of the physical documents that we all possess today, such as: plastic cards, passports, driving licenses, qualifications and awards, etc. After the computation of the data object, the next step involves generating a unique hash for the document. This hash serves as a digital fingerprint, uniquely identifying the document's content. The generated hash is then assigned and stored in a variable known as merkleRoot. This value is then recorded on an Ethereum compatible network for issuance proof, ensuring the document's integrity and providing a verifiable record.

```
{
  "version": "https://schema.openattestation.com/2.0/schema.json",
  "data": {
    "name": "2f1a9924-bc38-455c-b39e-6420001ad67b:string:Maersk Bill of Lading",
    "issuers": [
      {
        "identityProof": {
          "type": "40caddff-5cd4-477d-adf4-48dcd0a2d761:string:DNS-TXT",
          "location": "c15358f4-f0dc-41c8-abfb-0d030aae3233:string:imaginative-amber-ferret.sandbox.openattestation.com"
        },
        "name": "0de92429-f8d3-47a0-868f-154227a66f40:string:DEMO STORE",
        "tokenRegistry": "89c1f33c-121d-4622-a561-12fb400f2f3f:string:0x8194648f40ED07F841fA357Bf52CBE8D6d7ce48D"
      }
    ]
  },
  "signature": {
    "type": "SHA3MerkleProof",
    "targetHash": "11d456db211d68cc8a6eac5e293422dec669b54812e4975497d7099467335987",
    "proof": [],
    "merkleRoot": "11d456db211d68cc8a6eac5e293422dec669b54812e4975497d7099467335987"
  }
}
```


Figure 5 Open Attestation formatted document

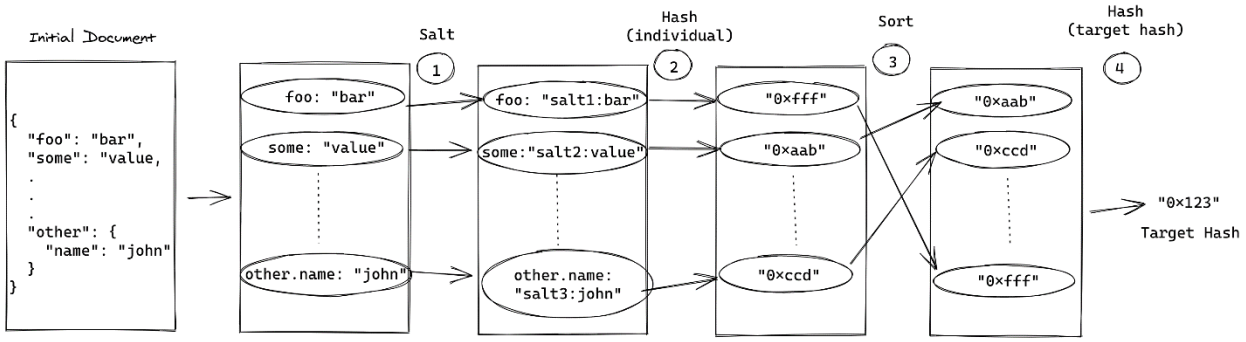

Figure 6 Mechanism of generating targetHash of the document

- Selective Disclosure: Selective disclosure enables the holder of Open Attestation formatted documents to present specific portions of the document for verification purposes. This functionality is accomplished by allowing users to conceal certain data fields while maintaining the overall integrity of the document. In order to implement this feature, a hash is computed over each individual hashed and salted key-value pair. When obfuscating data, the salted key-value pair is hashed, and the resulting hash is stored in a separate location within the document.

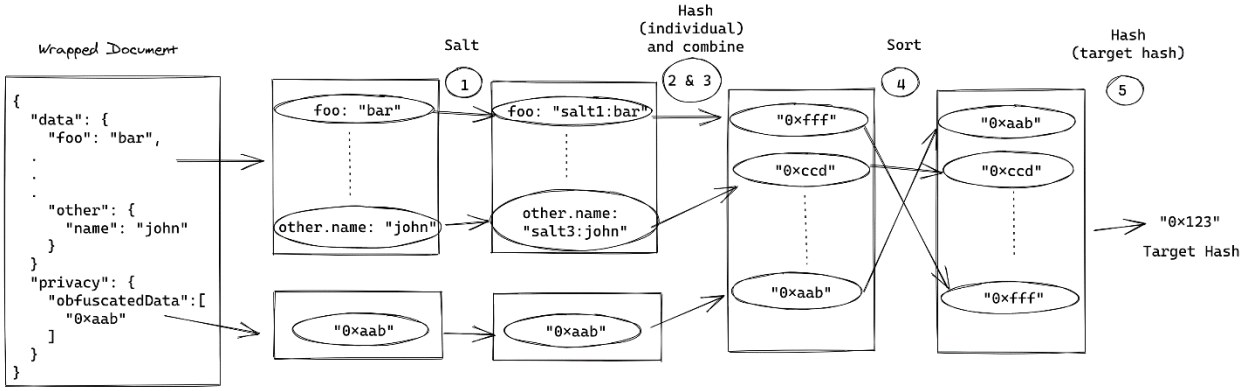

Figure 7 Mechanism of generating targetHash with selective disclosure

- The decentralized renderer: provides Open Attestation (OA) documents with a human-readable appearance. It functions as a website that takes the data of an OA document as input

and presents the document in a web view format. This enables users to customize the visual styling of their document without the need to submit code changes to a third party.

- Verified Issuer's Identity: The document store is a smart contract deployed on an Ethereum compatible blockchain network. It securely stores proofs of Open Attestation (OA) document issuance, providing a globally consistent record for querying the issuance status. To issue an OA document, a domain is required, and a DNS record is inserted to assert the identity of the document creator. This setup ensures trust and authenticity by leveraging blockchain technology and validating ownership of the domain through DNS records.

Type	Name	Value
TXT	example.com	"openatts net=ethereum netId=3 addr=`<DOCUMENT_STORE_ADDRESS>`"

Figure 8 Sample of dns TXT record

4.2.2. CamDL (Cambodia Distributed Ledger)

CamDL is a unique blockchain network that combines the characteristics of both permissioned and public blockchains. As a permissioned blockchain, it requires participants to obtain specific permissions in order to join the network and engage in transaction validation and block creation. This permissioned approach ensures a higher level of security and control compared to public blockchains.

The primary objective of CamDL is to offer the general public a robust platform for experimenting with and developing Web3 applications. Web3 applications refer to decentralized applications (dApps) that utilize blockchain technology and aim to solve everyday problems or contribute to the decentralized finance (DeFi) ecosystem.

By providing a platform for experimentation and development, CamDL aims to encourage innovation and creativity in the blockchain space. It allows developers and entrepreneurs to build and deploy their own dApps, leveraging the underlying blockchain infrastructure to create solutions that address real-world challenges.

Moreover, CamDL serves as a crucial component of the DeFi ecosystem. DeFi refers to the decentralized finance movement, which aims to transform traditional financial systems by utilizing blockchain technology. CamDL offers a foundation for DeFi projects by providing the necessary infrastructure and tools for developers to create DeFi applications.

With CamDL, individuals and organizations can explore the potential of blockchain technology, experiment with new concepts, and contribute to the growth of the Web3 and DeFi ecosystems. It fosters an environment of innovation and collaboration, empowering developers to build solutions that can have a meaningful impact on various industries and everyday life.

Within the eKYC (electronic Know Your Customer) interoperability system, CamDL plays a crucial role by providing a robust blockchain infrastructure that benefits all stakeholders

involved. One of the key participants in this system is the eKYC provider, who can leverage the blockchain network offered by CamDL to attest KYC information. This process ensures the verification and validation of customer identity details.

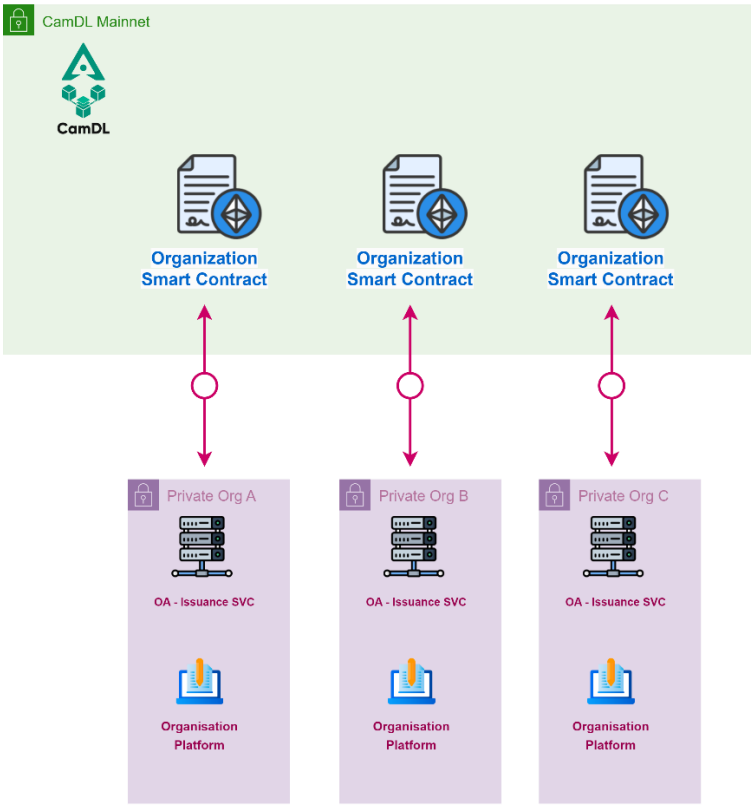

Figure 9 Organization ownership of smart contract within CamDL Blockchain Network

To achieve this, the eKYC provider can utilize this Open Attestation framework to generate an attestation for the KYC information, creating a digital proof of its authenticity and integrity. The attestation includes crucial details such as the customer's identity, proof of verification, and other relevant information.

Once the attestation is created, the eKYC provider publishes the merkleRoot value into their organization's smart contract. In this context, each organization involved in the eKYC interoperability system has its own separate smart contract, which provides them with full sovereignty and control over the attestation process.

The verifier, who is responsible for confirming the validity of the attested information, can utilize the CamDL blockchain infrastructure to conduct the verification process. By checking the integrity and the merkle root of the attested information against the records stored within the issuer’s smart contract, the verifier can ensure that the information has not been tampered with and that it has indeed been attested by the respective eKYC provider organization.

4.3. KYC Data Exchanges

In the eKYC interoperability standard, there is no enforced mechanism for data exchange between the eKYC provider and verifier. However, to ensure secure data exchange between these parties, the recommended solution is CamDX (Cambodia Data Exchange). CamDX, inspired by Estonia's X-Road model, serves as a platform that facilitates the confidential and secure exchange of data among various entities. By adopting CamDX, stakeholders can maintain the confidentiality, integrity, and interoperability of data when sharing it with multiple data exchange parties. This ensures that sensitive information remains protected while allowing for seamless collaboration and data exchange within the eKYC ecosystem.

4.4. Data Privacy and User consent

This document emphasizes the utmost importance of user data privacy within the eKYC ecosystem, particularly in the context of the eKYC interoperability standard. While the eKYC platforms possess user information, it is crucial that every utilization of this data strictly adheres to the user's explicit consent. The KYC platforms are responsible for implementing necessary measures to ensure that user consent is obtained genuinely and explicitly. This may involve additional steps such as OTP (One-Time Password) or PIN confirmation, which validate the user's consent before any data sharing takes place. By prioritizing these safeguards, the eKYC platforms uphold the principles of user privacy and reinforce the trustworthiness of the eKYC process.

4.5. API Economy

The eKYC interoperability standard introduces the opportunity for the KYC provider to charge fees to the requester organization for exchanging KYC user information. This financial arrangement allows the KYC provider to recover costs associated with user registration and verification, while enabling the requester organization to save on expenses related on establishing their own KYC solution to meet compliance requirements. However, the pricing of the API exchange is not mandated by the standard and is open to negotiation between the parties involved. Factors such as the amount of data required (KYC tiering) or authentication-only needs should be considered when determining the pricing agreement.

An organization can serve as both the provider of KYC information and the requester, offering increased flexibility in the eKYC process. This dual role enables users to register and authenticate seamlessly across various platforms, ultimately enhancing their digital adoption and overall user experience. By consolidating the roles of provider and requester, organizations can streamline the onboarding and authentication processes, minimizing friction and simplifying user interactions. This approach not only benefits users by providing a more unified experience but also empowers organizations to leverage existing KYC data efficiently, optimizing resources and improving operational efficiency.

4.6. KYC Quality and Acceptance

The interoperability standard outlined does not enforce mandatory acceptance between eKYC providers and requester organizations. Instead, it encourages organizations to exercise their own judgment and engage in collaborative efforts to enhance user experience and seize

collaboration opportunities. The decision to accept an eKYC provider lies with the respective organizations, allowing them to assess the compatibility, reliability, and suitability of the provider's services for their specific needs. This approach fosters a flexible environment where organizations can choose to collaborate with eKYC providers that align with their requirements, enabling them to optimize user experience, streamline processes, and foster productive partnerships based on their unique circumstances and objectives.

4.7. KYC Unified Data Template Standard

To facilitate seamless interoperability and compatibility across different organizations, the establishment of a standard Open Attestation data template is crucial. This unified data template serves as a standardized implementation that can be adopted by various organizations, ensuring consistency and harmonization in the eKYC exchange process. By adhering to a common data template, organizations can effectively exchange eKYC information regardless of the specific platforms or systems they utilize. This platform-agnostic approach eliminates the need for extensive modifications or customizations to adapt to different eKYC systems, resulting in a more streamlined and efficient data exchange experience. The standard Open Attestation data template promotes a unified framework for eKYC data sharing, enabling organizations to seamlessly collaborate and exchange information, ultimately enhancing interoperability and facilitating effective communication across the eKYC ecosystem.

The development of a common standard data template necessitates inputs from diverse and relevant organizations to ensure both backward compatibility and future-proofing of the standard. By actively involving multiple stakeholders, the aim is to establish a robust framework that minimizes the need for extensive modifications and remains adaptable to various use cases within enterprises. This collaborative approach ensures that the standard data template can effectively accommodate the evolving needs of organizations, enabling seamless integration and compatibility across different systems and platforms. By considering a wide range of perspectives and requirements, the standard can be designed to withstand future challenges and technological advancements, providing a strong foundation for long-term usability and versatility.

```
{
  "version": "https://schema.openattestation.com/2.0/schema.json",
  "data": {
    "$template": {
      "name": "RANDOM_UUID_V4:string:OPENATTESTATION_KYC_CAMBODIA_V1"
    },
    "id": "RANDOM_UUID_V4:string:UNIQUE_ATTESTATION_ID",
    "recipient": {
      "dateOfBirth": "RANDOM_UUID_V4:string:DATE_OF_BIRTH",
      "issueDate": "RANDOM_UUID_V4:string:ID_ISSUE_DATE",
      "expireDate": "RANDOM_UUID_V4:string:ID_EXPIRED_DATE",
      "gender": "RANDOM_UUID_V4:string:M_F",
      "nationality": "RANDOM_UUID_V4:string:NATIONALITY",
      "firstName": "RANDOM_UUID_V4:string:FIRST_NAME",
      "lastName": "RANDOM_UUID_V4:string:LAST_NAME",
      "idNumber": "RANDOM_UUID_V4:string:ID_CARD_NUMBER",
      "selfie": "RANDOM_UUID_V4:string:SELFIE_IMAGE_BASE64",
      "idImage": "RANDOM_UUID_V4:string:ID_CARD_IMAGE_BASE64"
    },
    "issuers": [
      {
        "documentStore": "RANDOM_UUID_V4:string:ORGANIZATION_SMART_CONTRACT_ADDRESS",
        "identityProof": {
          "location": "RANDOM_UUID_V4:string:ISSUER_DOMAIN",
          "type": "RANDOM_UUID_V4:string:DNS-TXT"
        },
        "name": "RANDOM_UUID_V4:string:ISSUER_NAME",
        "url": "RANDOM_UUID_V4:string:https://ISSUER_DOMAIN"
      }
    ]
  },
  "signature": {
    "type": "SHA3MerkleProof",
    "targetHash": "CALCULATED_HASH_OF_DOCUMENT",
    "proof": [
      "TARGET_HASHES_DOCUMENT_IN_BATCH"
    ],
    "merkleRoot": "MERKLE_ROOT_ATTESTATION"
  },
  "privacy": {
    "obfuscatedData": [
      "HASHES_OF_HIDDEN_FIELD"
    ]
  }
}
```


Figure 10 Sample of eKYC attestation standard template

5. Key Stack Holders' Definition

5.1. Data Owner (End User)

Data owners are individuals who voluntarily enroll themselves in various platforms. Despite providing their data to these platforms, they retain full rights and control over their own information. It is imperative to empower data owners by offering them the opportunity to utilize their own data for registering or authenticating themselves on other platforms, thereby enhancing their personal benefits and convenience.

5.2. eKYC Provider

eKYC providers are organizations that users voluntarily enroll themselves into. These platforms offer users a dedicated platform to register their information and subsequently verify the accuracy of the provided data. While the eKYC providers have access to user data, it is crucial for them to adhere to strict guidelines when using or sharing this information. The platform is obligated to clearly state the specific details being accessed or exchanged and ensure that explicit consent is obtained from the user.

5.3. eKYC Requester

eKYC requesters are platforms that users choose to enroll in. Rather than filling out all the required information, users have the option to utilize the eKYC results obtained from an eKYC provider for quick and efficient enrollment or authentication purposes. It's important to note that although the roles are defined separately, an organization can potentially fulfill both the provider and requester roles within the eKYC ecosystem. This flexibility allows organizations to leverage existing eKYC data while simultaneously benefiting from the convenience and speed of the eKYC process.

5.4. eKYC Interoperability Standard Operator (Techo Startup Center)

Techo Startup Center (TSC) is the eKYC Interoperability Standard operator. It's important to note that TSC does not have access to user information as the data exchange occurs solely between the requester and the provider. TSC's primary responsibility lies in overseeing the standard itself, ensuring its effective implementation, and facilitating continuous improvements. To achieve this, TSC actively engages with relevant stakeholders, gathering valuable input and feedback to enhance the standard's functionality, security, and usability. In addition, TSC serves as a valuable resource for organizations seeking to integrate the eKYC Interoperability Standard into their systems. They provide comprehensive integration guidance and offer necessary tools and resources to support successful implementation. By assuming these roles, TSC plays a critical role in promoting the adoption and advancement of the eKYC Interoperability Standard, fostering a cooperative environment among stakeholders, and driving innovation within the eKYC ecosystem.

5.5. CamDL Operator (Techo Startup Center)

Techo Startup Center (TSC) assumes the role of the operator for the CamDL blockchain network. It's important to emphasize that CamDL maintains a strong commitment to user privacy, as it does not have access to user information. TSC is responsible for ensuring the stability and robustness of the blockchain network. To achieve this, TSC actively seeks additional validators or RPC nodes to enhance the network's availability, trustworthiness, and overall performance. TSC also places a significant emphasis on maintaining the immutability of the blockchain records, ensuring they remain unalterable and resistant to tampering. In addition to network management, TSC provides on-demand compute credits to organizations interested in exploring or utilizing the capabilities of the CamDL blockchain network. This

offering enables organizations to seamlessly test and integrate with the blockchain network, promoting innovation and facilitating the exploration of its potential applications. Through these endeavors, TSC supports the secure and reliable operation of the CamDL blockchain network, fostering trust, accessibility, and immutability for all participants.

6. How it works

The eKYC sharing process is divided into five main steps:

6.1. Obtaining First Digital eKYC Result

The first step in the eKYC sharing process involves the user's initial registration with any eKYC provider. During this registration, the user follows the traditional approach of inputting their information, which may include submitting relevant documents or providing biometric data. In cases where the user is already registered with the eKYC provider, this step can be skipped.

After the user completes the eKYC process, the eKYC provider proceeds to attest the eKYC result for that specific user. This attestation is typically in the form of an Open Attestation document, which serves as a digital proof of the user's verified identity information. The eKYC provider then stores the hash of this attestation document on the blockchain network, ensuring its immutability and tamper-proof nature.

Once the eKYC result is attested and stored on the blockchain, the user can leverage this verified information for future interactions. They can reuse the eKYC result to register or authenticate themselves on various platforms that collaborate with the eKYC provider. By reusing the attested eKYC result, the user can streamline the registration and authentication processes, eliminating the need for repetitive data submission and verification.

6.2. Registration or Authentication Request

When a user intends to perform registration or authentication on any platforms, they can leverage the eKYC standard to streamline the process. In this scenario, the requester platform plays a crucial role by providing essential information related to the request. This includes details about the specific eKYC mechanism being employed, the template for the Open Attestation document, a sessionId for tracking purposes, the mechanism for exchanging data, and a callback URL for result callback.

The eKYC request can be initiated in two different ways depending on the user's context. If the user is accessing the requester platform through a mobile app, the eKYC request can take the form of deeplinking. On the other hand, if the user is accessing the requester platform via a web portal, the eKYC request can be initiated through a QR code. This approach ensures a smooth and convenient user experience, enabling users to seamlessly navigate between different platforms while maintaining the necessary security measures for eKYC processes.

```
{
  "type": "KYC_INTEROP_STANDARD_OA",
  "sessionId": "UNIQUE_SESSION_ID",
  "template": "OPENATTESTATION_KYC_CAMBODIA_V1",
  "endpoint": "https://REQUESTER_CALLBACK_URL",
  "exchangeMode": "CAMBODIA_CAMDX"
}
```


Figure 11 QR or Deeplink Payload

6.3. Choosing Provider eKYC and User Consent

When initiating a data request for eKYC purposes, the user is presented with the option to select a KYC provider from a list supported by the requester system. The selection can be made either through deep linking or QR code scanning, depending on the available platforms supported by the requester. Once the user chooses their preferred method, the eKYC provider takes charge of specifying the specific data to be shared with the requester platform. This ensures that only relevant and necessary information is exchanged.

In order to prioritize user consent and data privacy, the eKYC provider incorporates an additional layer of security. This typically involves obtaining explicit user consent for data sharing, often through an OTP (One-Time Password) or PIN confirmation process. By implementing these measures, the eKYC provider ensures that user data is shared with the requester platform only after the user has confirmed their consent, thereby maintaining a high level of security and user control throughout the eKYC process.

Upon receiving and confirming user consent, the eKYC provider proceeds with the data exchange process. To enable the requester organization to retrieve user information, the eKYC provider provides them with a JWT (JSON Web Token). This token serves as a secure authorization mechanism, granting the requester organization access to the specific user data as permitted by the user's consent. By utilizing the JWT token, the requester organization can securely retrieve the necessary information from the eKYC provider, ensuring a smooth and controlled data exchange process.

6.4. Information Retrieval, Verification and Enrollment

The requester organization utilizes the acquired JWT token to initiate a request for user information. Once the user information is obtained, typically in the form of Open Attestation format, the requester organization proceeds to verify the content of the information. This verification process ensures the immutability and proof of issuance from the issuer organization. Leveraging technologies such as blockchain and DNS records of the issuer institution, the requester organization establishes the authenticity and integrity of the user information. Upon successful verification, the user can then be enrolled or authenticated into the platform based on the provided and validated information. This robust verification mechanism enhances trust and security in the enrollment and authentication processes.

7. Prototyping

The document includes an early prototype to showcase the technology's functionality for end users. It also provides details on the system's interactions to achieve efficient and secure eKYC data exchange.

7.1. User Journey (UI/UX Prototyping)

The prototype covers a scenario involving Mr. Mean Somnang, who has registered an account and completed KYC verification with Mango Bank. Mr. Somnang intends to register with Apple Bank and seeks to streamline the process by utilizing the verified KYC information obtained from Mango Bank. To achieve this, he employs the eKYC interoperability standard, allowing him to seamlessly complete his registration with Apple Bank.

7.1.1. Mobile Prototyping

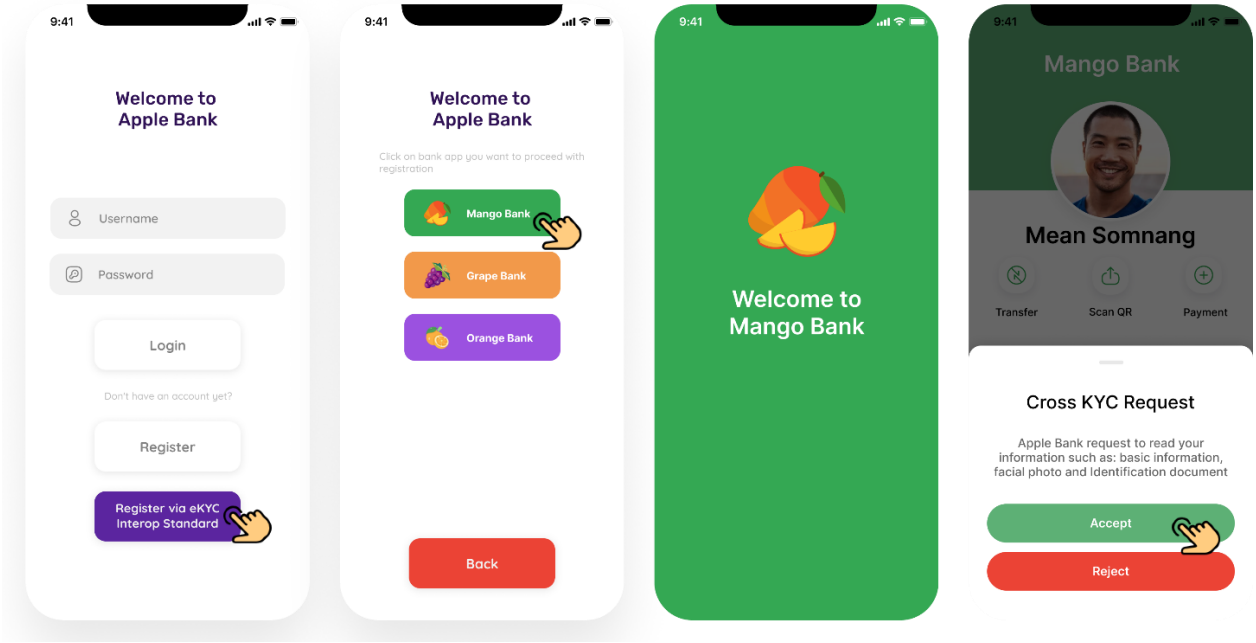

Figure 12 Mobile Prototyping (Part 1)

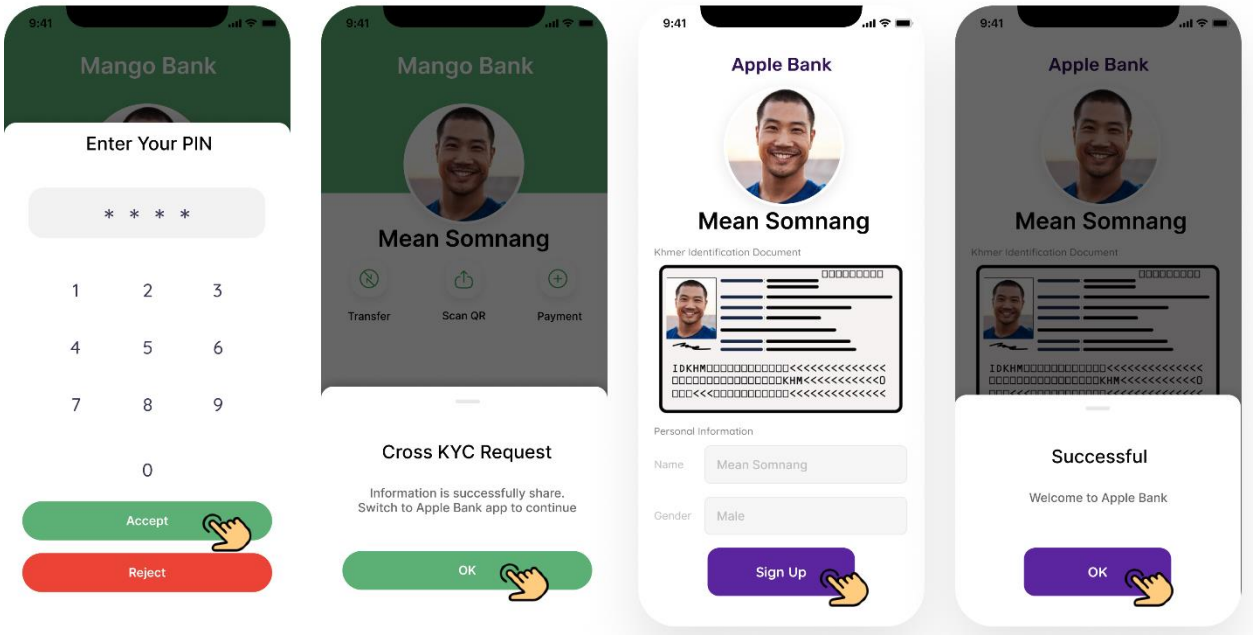

Figure 13 Mobile Prototyping (Part 2)

7.1.2. Web Prototyping

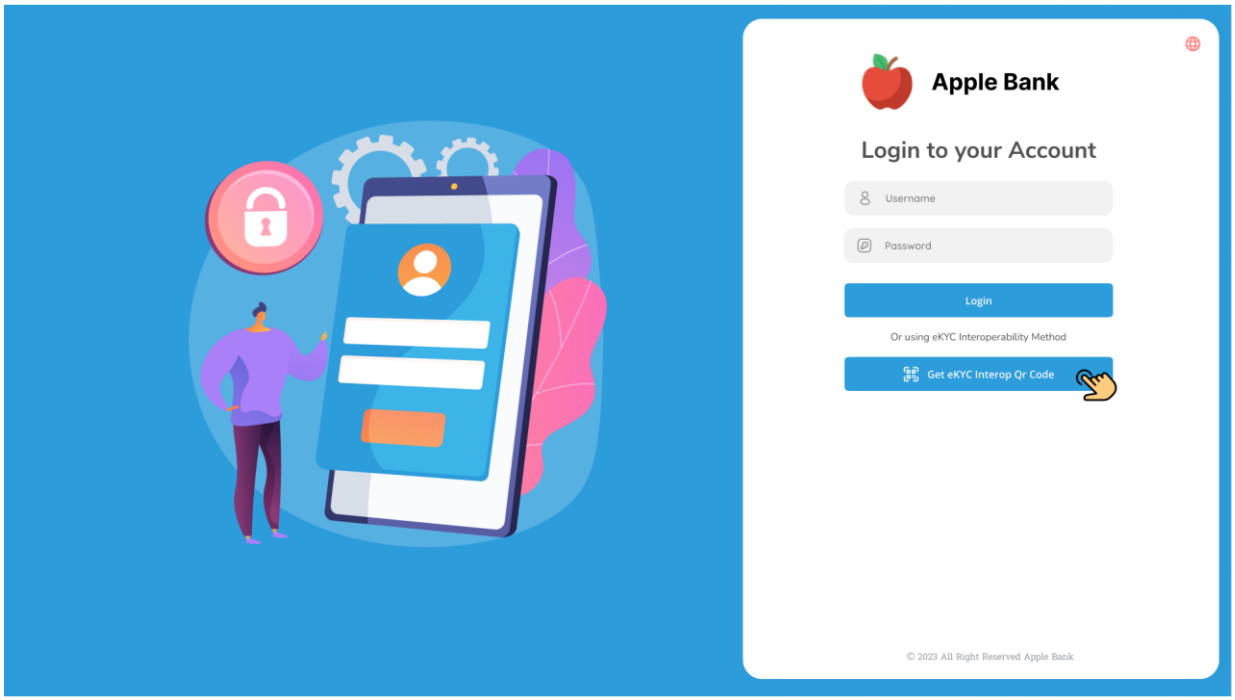

Figure 14 Web Prototype eKYC Interop (part 1)

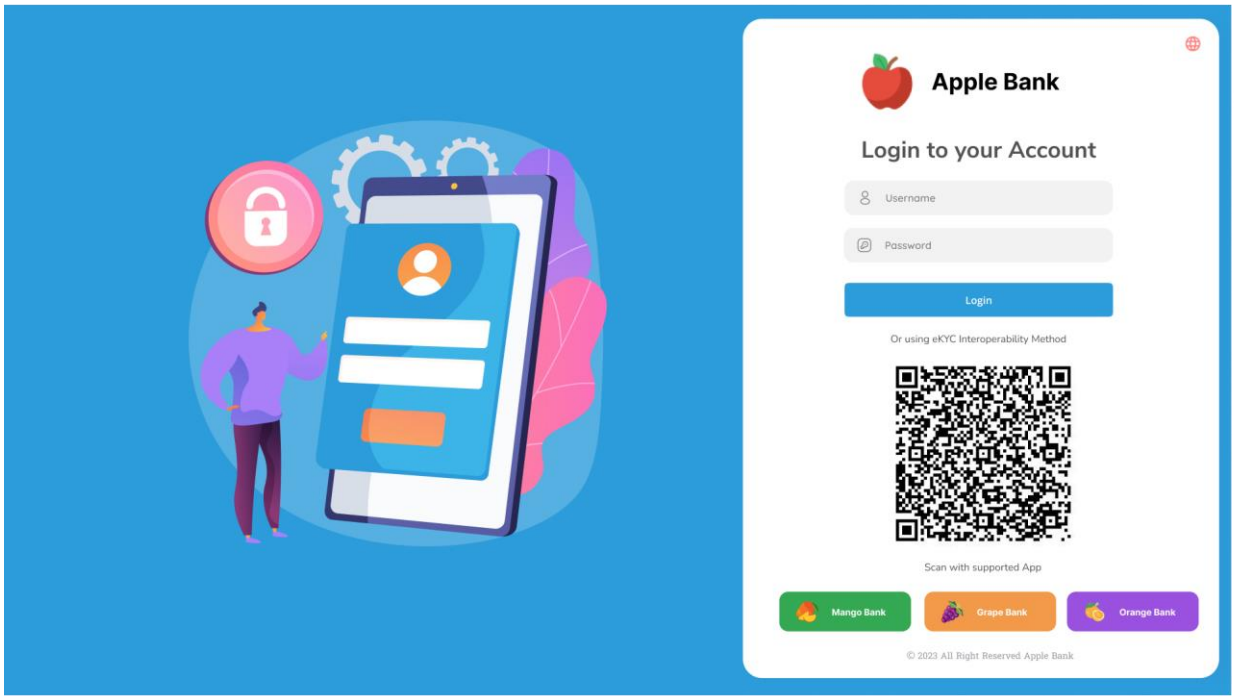

Figure 15 Web Protoype eKYC Interop (part 2)

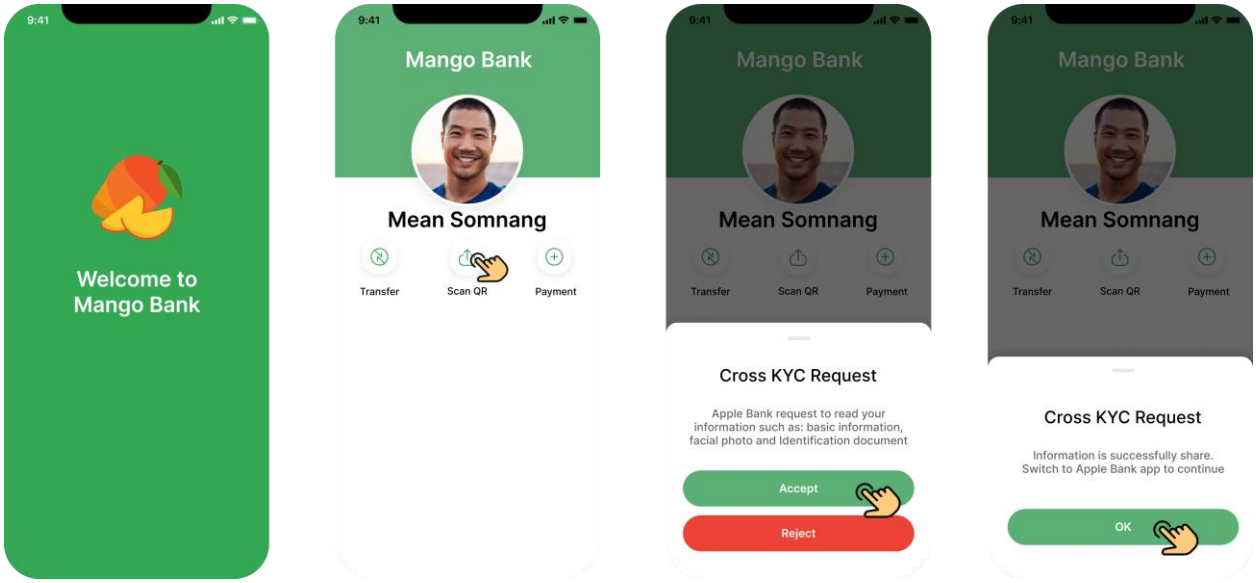

Figure 16 Web Prototype eKYC Qr Scan by Mobile App (part 3)

7.2. System Flow (System Prototyping Design)

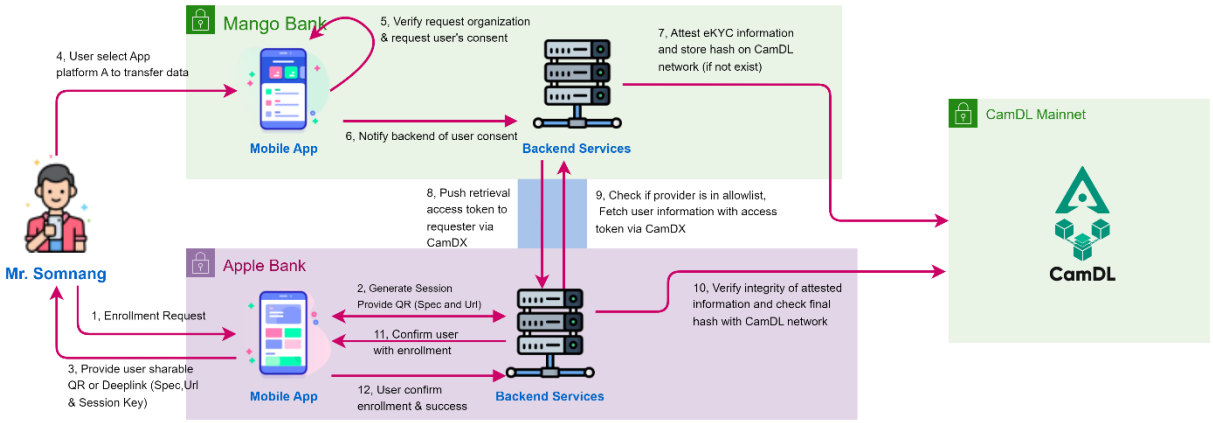

Figure 17 Full system flow of the eKYC Interoperability Standard

7.3. Issuance and Verification Service

Organizations have the option to implement issuance and verification using the Open Attestation Framework directly or by leveraging the services offered by the Techo Startup Center. To begin utilizing this technology, please visit: https://github.com/Techo-Startup-Center/openattestation-issuing-svc

Figure 18 Qr Link to attestation and verification service and document

TECHO STARTUP CENTER