UQUDO'S PLATFORM

White Paper

Business Contact Information

Contact Details:	Uqudo Technology Limited
Phone:	+971 455 43646
Email:	hello@uqu.do
Address:	Office 8, Level 4, Gate 05 Dubai International Financial Centre Dubai PO Box: 120252 UAE

Confidentiality Notice

Notwithstanding anything to the contrary, this white paper and associated documents contain confidential and proprietary information, and shall not be disclosed without the prior written consent of uqudo. This document is non-binding and shall be used for discussion purposes only.

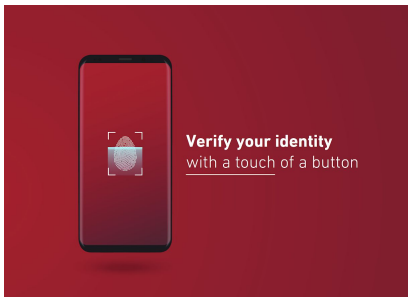
While every effort will be made to ensure that the information contained in this response is accurate, uqudo makes no warranty or undertaking expressed or implied, that this submission is accurate and complete; any product roadmap features and delivery dates that may be mentioned in this document represent current product development expectations only, and not a commitment.

1. Introduction

Organisations are looking increasingly to digitise their operations. At uqudo, we understand how to embed technology in processes and services. We deliver exciting digital acceleration technology whilst supporting the speed of business. We provide a powerful business transformation solution that creates more opportunities to capture additional market share.

Many organisations in today's world are looking to provide improved customer experience whilst delivering their customers' requirements. We translated these requirements to an agile solution with defined success criteria:

- Data accuracy as an imperative factor
- A simplified customer journey - provisions for a comprehensive frictionless onboarding experience
- Cost savings on functions throughout the customer value chain and management of policies
- Time-saving process across the user experience



uqudo has delivered, and is in the process of delivering, major projects ranging from startups to multinational organisations. Within the IAM security domain, uqudo is very familiar with the security and confidentiality measures regarding the management of identities.

مبادرات محمد بن راشد آل مكتوم العالمية
Mohammed Bin Rashid
Al Maktoum Global Initiatives

مؤسسة محمد بن راشد آل مكتوم للمعرفة
MOHAMMED BIN RASHID AL MAKTOUM
KNOWLEDGE FOUNDATION

uqudo's platform is the proud winner of the Arab Innovation Startup Award for Technology 2018 organised by Sheikh Mohammed Bin Rashid Al Maktoum Knowledge Foundation, formed by His Highness Sheikh Mohammed Bin Rashid Al Maktoum.

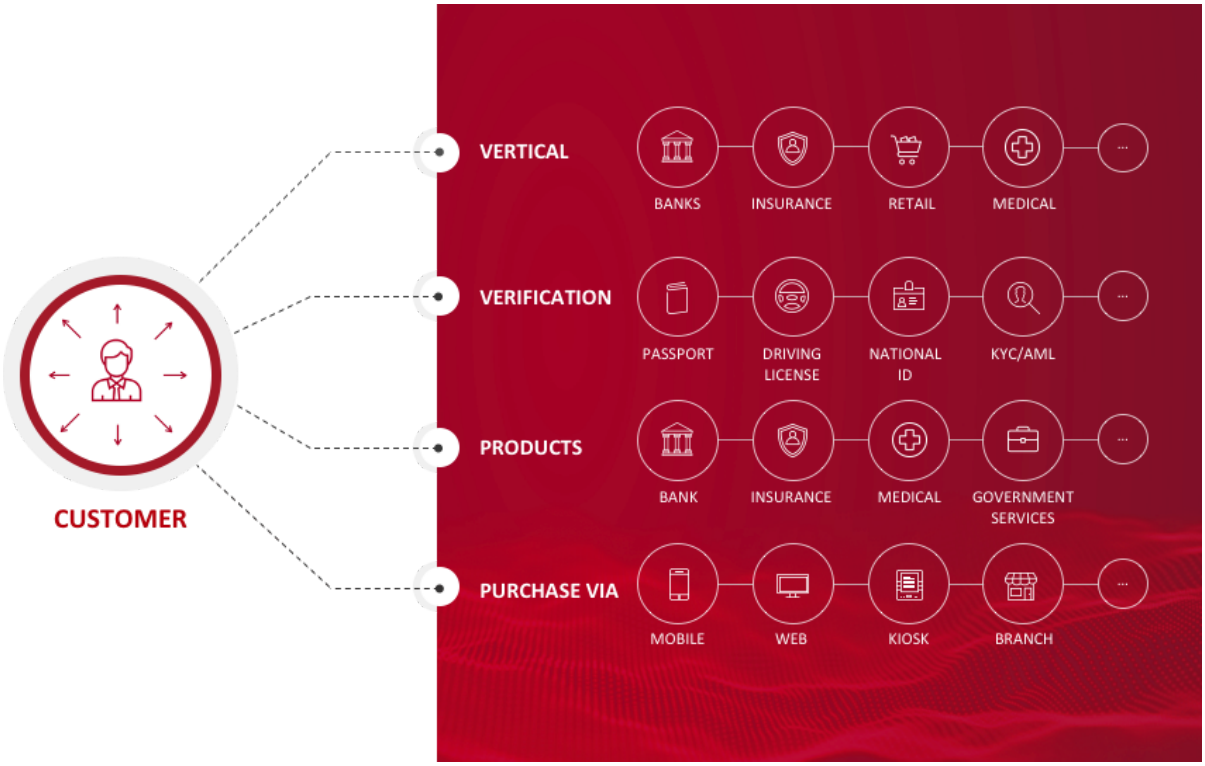
uqudo - the most innovative digital identity company in the Middle East and Africa.

2. Synopsis

uqudo offers a platform which will be used as an IDaaS (Identity as a Service). It will enable the capture of an authentic identity which will permit each of your customers to be unique thus preventing a duplicate account with another pseudo or identity.

This unique and seamless solution provided by uqudo will eliminate time consuming and heavy administration processes including removing the need for physical documents to be signed/stamped/approved by KYC in the back office. This leads to a flawless and frictionless experience for the customer.

The additional and important value within this unique standard onboarding is that customers do not need to provide their details again for other products/services related to your service. Customers have a unique profile and a document vault that enables them to reuse verified documents and attributes to consume new products without the need of repeating the process. This can be achieved regardless of the channel or geographical location used by the customer.



3. uqudo's Digital Experience

uqudo provides a platform for identity management that maintains the complete lifecycle of an individual's interaction with a single or multiple organisation(s). The platform has its own identity validation and verification capabilities but it is also pluggable into a number of identity verification platforms. The platform has been built with common use cases and requirements embedded within it, making it flexible and inclusive to other vendors and organisations to incorporate it within their processes.

Onboarding

Sharing & Blockchain

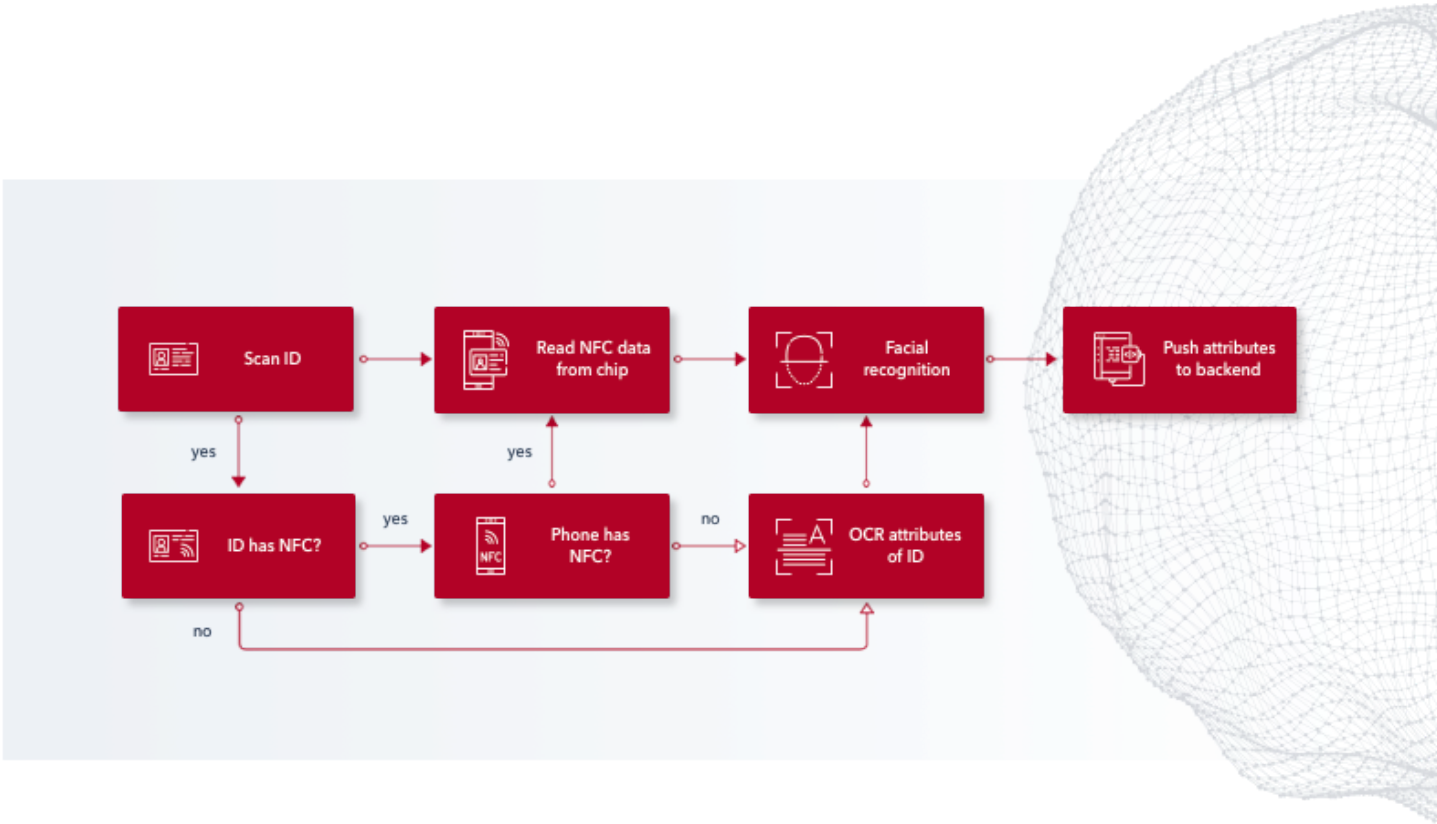
Authentication

The platform provides three major use cases Onboarding, Sharing and Authentication. Onboarding covers the end-to-end flow of user registration, the validation of ID documents and background screenings. Sharing covers the distribution of customer details and KYC information with affiliates with the consent of the user, in compliance with data privacy regulation. Authentication covers the process of verifying the identity of users that are already onboarded. The users will authenticate using biometrics instead of passwords or security questions.

uqudo will work with your organisation to enable the use case that will be required for the current and future evolution of your business. We believe that uqudo is the right partner to work with you on new propositions that will facilitate any iterations.

3.1. Onboarding

The mobile phone technology has evolved vastly over recent years. Users can now use a smartphone to create assured digital accounts.

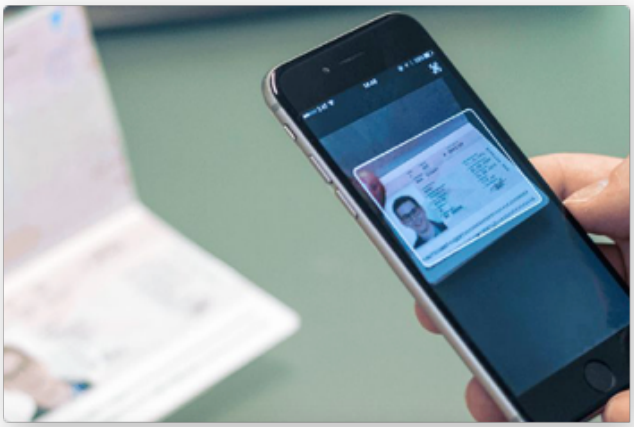


The process scans the ID, reads NFC data, performs facial recognition and then post-proofing the identity of the user, creates an account with verified data. However not all phones currently support NFC and nor do all ID documents have an NFC chip. The diagram above depicts the alternative processing route route taken to accommodate this.

100% coverage can be achieved by combining both process paths and is fully automated. The journey is wholly transparent to the users as the solution can detect if the phone has an NFC reader and whether the ID document supports NFC. Over time more ID documents and mobile devices will be embedded with NFC chip technology reducing the requirement for OCR usage.

The process flow taken by the user is captured with its metadata. This data collection will provide a trust factor and a score for the transaction. uqudo is working to further develop this with an element of AI and machine learning, to give a calculated more targeted risk factor number.

The uqudo platform offers a fully automated process to onboard ID documents in an efficient and secure way with three easy steps:



Step 1: **Scan the ID document**

The users use a mobile app that includes the uqudo SDK to scan their ID document (e.g. Passport). The SDK supports both one-sided ID documents such as passports and two-sided ID documents such as an Emirates ID. During the scanning, the SDK extracts the data including MRZ, QR codes, PDF417 codes, bar codes and the facial image. It also can provide a document image.

Step 2: **Read the NFC chip of the ID document**

The phone reads the ID document data including the picture from the chip. The data is digitally signed. The backend of the uqudo SDK validates the certificates to ensure the data read is genuine. This step is applicable for NFC-enabled phones and biometric ID documents.

Step 3: **Perform a facial recognition**

The app performs facial recognition to verify the owner of the ID document is performing the onboarding. The facial recognition step only requires a phone with a selfie camera. The process also includes liveness detection which ensures the selfie captures a real person and not a photo or a video held in front of the camera.

Once the user completes the steps. the captured data is pushed securely to your organisation. Optionally, the SDK can calculate the hashes of the data and put them on the blockchain to ensure the integrity of the captured data. The hashes can be used at a later point to verify the ID document data.

3.2. Sharing & Blockchain

uqudo offers a unique way to store various IDs in an ID digital wallet. The wallet manages data stored on the phone and complies with GDPR and strict data privacy laws. It enables the user to take control of their data and share it with consent. The wallet will enable the ease of integration with other organisations that either store, process or transmit the identity. An example is the sharing of verified data with a third party after triggering the user consent and vice versa.

Identity Wallet

Card Details

Users can load physical ID cards into the wallet. The screens above show the identity wallet with a collection of all ID cards. The wallet is based on SDKs (Software Development Kit) and can be integrated with any existing mobile app. Users can enrol ID documents and profiles as described above to build their digital profiles. Each person is represented as a card that shows a number of attributes. The layout of a card can be designed by the card issuer including the logos and the attributes.

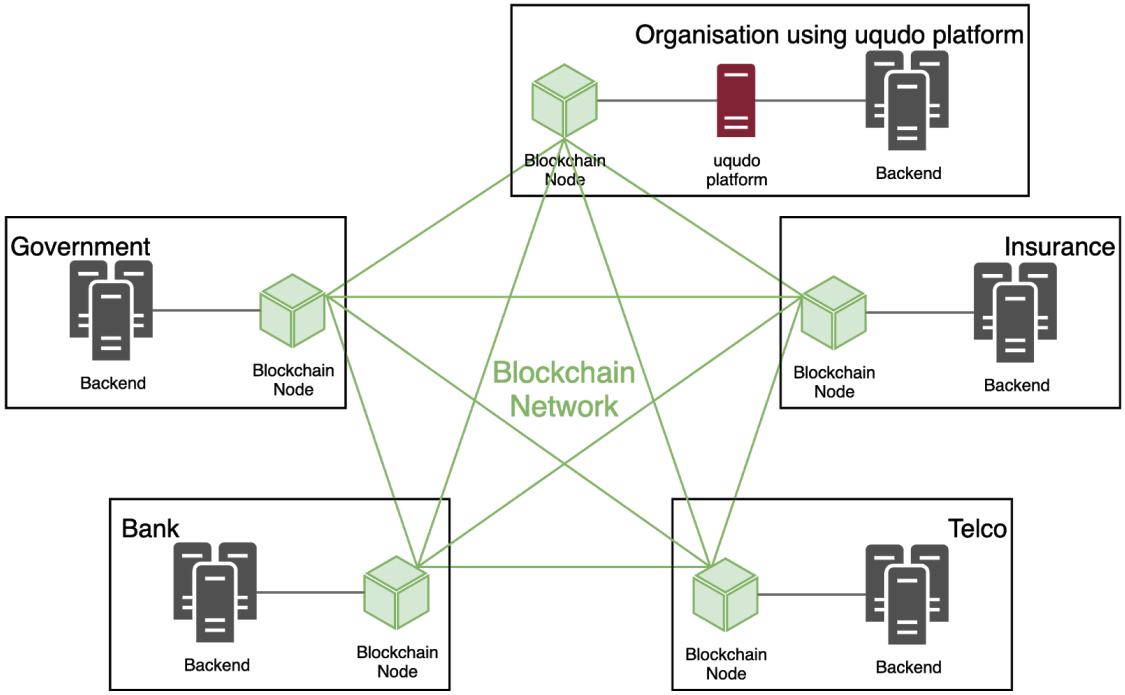
When the user selects one of the cards, the card details are shown as depicted above. The screen shows all attributes of an ID Card. Users can share the ID cards with affiliates to consume other services that require verified personal data. There are a number of mechanisms to share the ID Card when using services:

- **QR code**: An ID card consumer scans the QR code to load an ID card to validate it
- **NFC:** The user sends the ID Card to a card consumer via NFC
- **Geolocation + time window**: The ID card consumer presses a button “send”. The Card Consumer presses a button “receive”. Based on the geolocation + time, a service in the background connects the right sender with the right receiver. The ID Card will be sent through the ID Card consumer mobile Internet.

Blockchain

The platform has capitalised on the blockchain data and this feature can be enabled to provide an extra layer of security and facilitate more rich use cases around data sharing and consent. The ID wallet is integrated with permissioned and public ledgers. No data is stored in the blockchain and the solution is compatible with data privacy laws and GDPR.

The uqudo platform only stores hashes and public keys on the blockchain. It ensures compliance with data privacy regulations while protecting the integrity of the shared data. The uqudo platform is blockchain agnostic and works with both private and public blockchain. The platform currently supports Hyperledger Fabric, Quorum and Ethereum. Other blockchain platforms are possible if required.



The illustration above gives a high level overview of the integration of the blockchain network. The blockchain network can have various participants such as banks, insurances, telcos and government agencies. Each participant operates a blockchain node. The blockchain node is connected with the backend through an interface. An example of how the solution works is the following:

A customer onboards with a bank:

1. Customer installs the bank app on their phone and starts the onboarding process
2. Customer onboards their national ID
3. uqudo platform verifies national ID and initiates bank's KYC and AML processes
4. uqudo platform calculates the hashes of the ID attributes and stores them in the blockchain
5. uqudo creates a digital representation of the national ID inside the Identity Wallet
6. uqudo creates a digital representation of a bank ID that confirms the KYC
7. Bank opens/activate account for customer

A week later, the same person wants to open a mobile wallet with a car insurance company:

1. Customer installs the insurance app on their phone and starts the onboarding process
2. Customer onboards their driving license and car registration
3. Customer presents the national ID, driving license and car registration cards stored in the customer vault app to the insurance app
4. The insurance firm receives the digital documents
5. Insurance firm verifies the attributes with the blockchain
6. Insurance firm activates the policy
7. The customer doesn't need to onboard any document again. All documents will be stored in the wallet.

The advantage is that the insurance firm receives a verified digital ID of the customer, which can also benefit from the KYC process.

3.3. Authentication

Once users are onboarded, they need to be authenticated before each interaction with your organisation. Users enrol their biometrics on their devices before access - no passwords are required. Biometric authentication works for both native mobile apps and websites opened on phones or desktop.

Some of the most common biometric authentication methods are:

- Face (Face ID/Liveness Detection)
- Fingerprint (Touch ID)
- Palm
- Iris
- Windows Hello
- External Tokens

Biometric authentication includes device management allowing users enrolled on one device to add additional devices to their account:

1. User onboards using a smartphone and enrols their fingerprint
2. User wishes to log in to the website from their desktop PC
3. User scans a QR code on the login screen using the enrolled phone and successfully logs in.
4. Website recognises that the user is logged in from a new device and offers to enrol biometrics on the new device.
5. User agrees and enrols with Windows Hello Face.

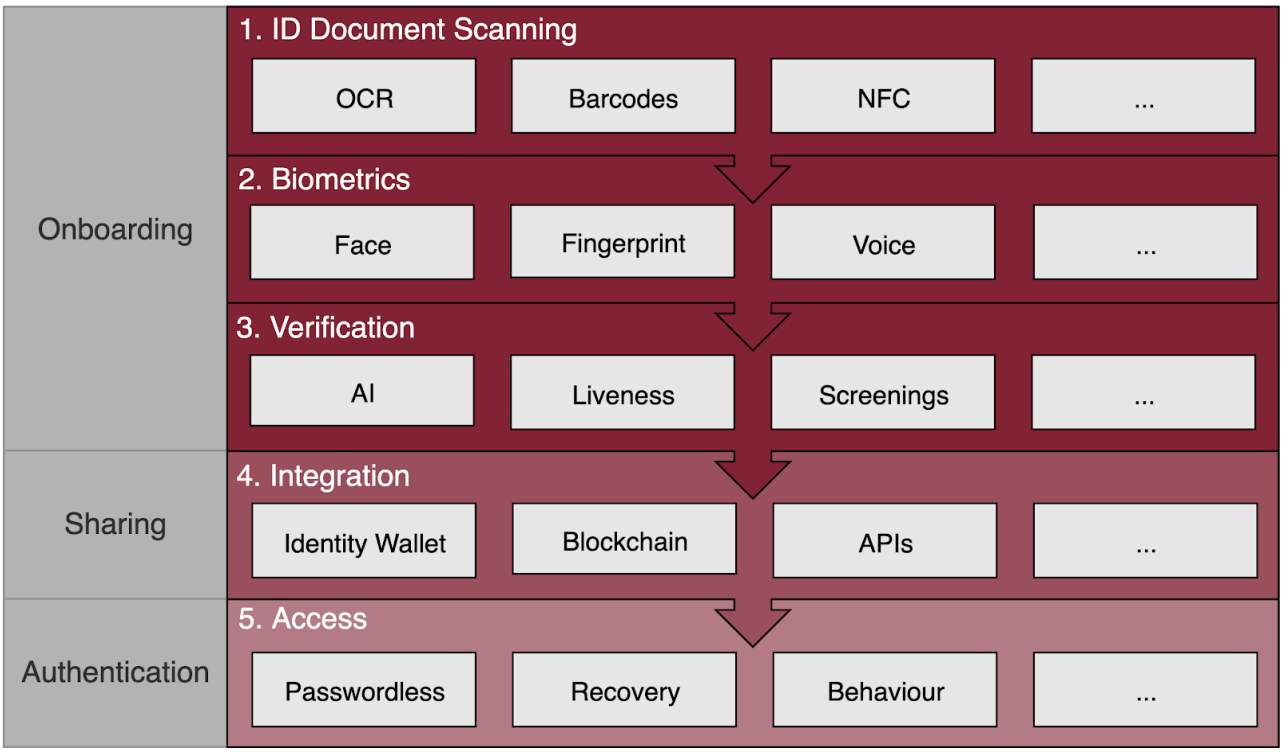
The user can now successfully log in to the website using their face. The technology is based on the FIDO (Fast ID online) standard and can easily be extended to other channels including:

- Kiosks
- Smart Speakers and Home Assistants (e.g Alexa)
- Authentication of IOT devices
- Smart Devices such as Wearables
- Interactions with Chatbots
- Call Centres
- ATMs

Account Recovery

If users need to recover their account (e.g. after device reset) they can easily do so without calling the service line or entering security questions. The requirement is to perform another face authentication which will be compared to the picture captured during the initial onboarding.

4. uqudo Platform



The figure above depicts the layers of the uqudo platform. It has 3 main features: onboarding, sharing and authentication. Each feature has one or more layers to provide the feature. The functionalities within each layer will be provided as modules. The uqudo platform is future-proof as it is effortless to include emerging functionalities by adding or replacing modules. This makes it possible to merge other solutions already in use by your organisation.

4.1. ID Document Scanning

ID document scanning is the process of capturing all-optical information from the ID document. uqudo supports the reading of the biometric chips that are embedded within documents using the NFC.

uqudo supports many document types including:

- National IDs
- Passports
- Driving licenses
- Car registration cards
- Company-related documents

The system can be trained to accept other required documents.

OCR

The uqudo module supports optical real-time capturing and verification. It includes optical character recognition (OCR) to read the attributes of a document including the Machine Readable Zone (MRZ). In addition, the optical face image can be extracted. The module can also capture a photo of the entire document (front and backside).

Barcodes

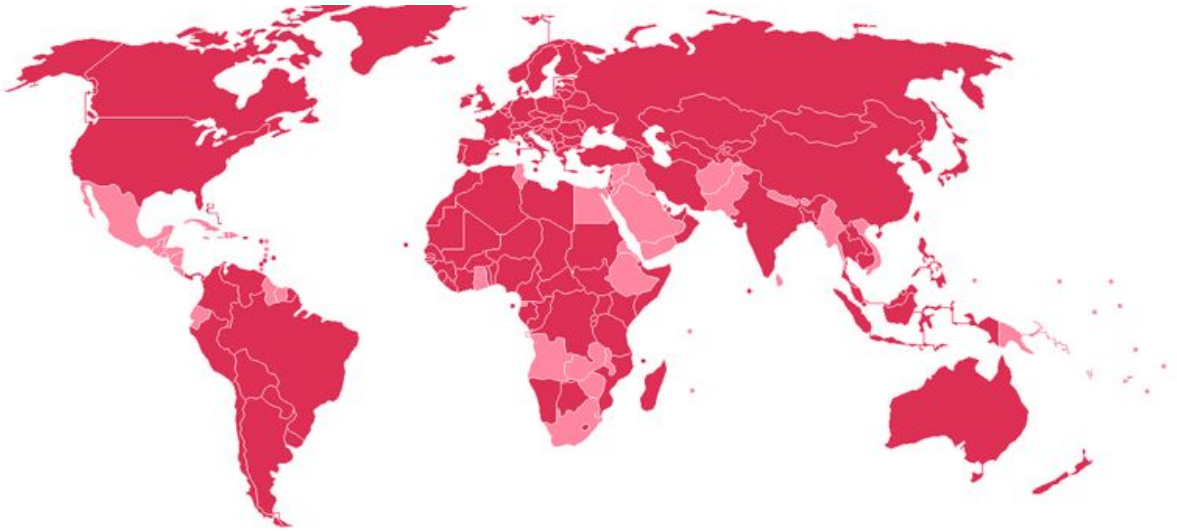
A barcode is a method of representing data in a visual machine-readable form. The module supports the interpretation of various barcodes such as:

- PDF417
- QR codes
- EAN

NFC scanning

An increasing number of documents include an NFC chip with identity data. The data include biometrics such as fingerprint or face. Modern smartphones are built with embedded NFC readers that are able to read the NFC data from ID documents. Generally, the data on the NFC chips is digitally signed by the issuer (e.g. country) to ensure the integrity of the data. The uqudo platform currently supports a vast number of national IDs and biometric passports whilst continuously adding to an increasing repository. It is simple to add additional NFC enabled ID documents to the platform if required.

Passports



Source: Countries issuing biometric passport according to Wikipedia

Many countries are issuing biometric passports through embedded NFC chips as depicted above. Document and chip characteristics are documented in the International Civil Aviation Organization's (ICAO) Doc 9303. The ICAO defines the biometric file formats and communication protocols to be used in passports.

The NFC Passport feature of the uqudo platform works in accordance with ICAO Doc 9303 MRTD. It includes:

- Basic Access Control
- Active Authentication (AA)
- Supplemental Access Control (SAC/PACE)

The uqudo SDK reads the chip to retrieve the facial image and details such as:

- Issuing country or organisation
- Surname
- Given names
- Passport number
- Nationality
- Date of birth
- Gender
- Passport expiry date

All data is digitally signed by the issuing country. The certificates published by countries are stored in the uqudo backend to verify the digital signatures and to ensure the integrity of the data.

National ID

Many national IDs, residence cards and driving licenses ship with an embedded NFC Chip. These kinds of IDs usually provide a rich set of attributes including personal details and a facial image.

The uqudo platform is able to read the fields by using the NFC reader of the phone. The uqudo platform is able to verify the signatures of the attributes to ensure the data is genuine. In addition, the platform can connect to the issuing entity to verify if the ID card has been reported lost or stolen.

4.2. Biometrics

The uqudo platform provides different options to ensure the person who onboards the document is the owner of the documents.

Face
The uqudo platform is capable of identifying and verifying a person from the image extracted from the ID document. The facial authentication algorithm compares selected facial features captured from the camera of the device with the extracted image. The algorithm uses biometric artificial intelligence to verify the person by analysing patterns based on the person's facial textures and shape. The algorithm also performs liveness detection to ensure a live person onboards the document to prevent presentation attacks such as photos, videos or masks.

Fingerprint
Where an external fingerprint reader is available, the uqudo platform can use fingerprint recognition software to confirm the identity of the person. External readers are available for both desktop pc and mobile devices. The uqudo platform can use the fingerprint template of supported ID documents to perform the verification.

Voice
Voice biometrics identifies a person through their unique voiceprint. Each person’s voiceprint is created based on the physical characteristics of the throat and mouth and this is then used by the system to validate their identity on subsequent phone calls. No two voices are the same; even identical twins have

different voice patterns. Because of the unique nature of voice, it can serve as a password, facilitating authentication processes and decreasing the risk of fraud.

4.3. Verification

After the capturing of identity data, verification is required to ensure the integrity of the data, detect any fraudulent actions and perform background checks.

AI

uqudo uses artificial intelligence (AI) to identify whether ID documents are genuine. Using machine learning creates a more efficient and accurate process than relying on an untrained human to look at ID documents. The algorithm has been trained to work with many documents. For example, the module can detect if a scan is a real document or just a copy on a piece of paper. The uqudo platform performs the verification in real-time during the onboarding process without any human interaction. These checks are tightly coupled to the capturing process.

Liveness

The goal of liveness detection is to determine if the biometric being captured is an actual measurement from an authorised, live person who is present at the time of capture. Liveness detection is based on recognition of physiological information as signs of life from:

- liveness information inherent to the biometric
- additional processing of information already captured by a biometric reader
- the acquisition of life signs by using additional hardware.

Liveness detection also includes challenge/response, where the user will see, hear or feel something and be required to respond verifying the liveness of the user.

Screenings

The uqudo platform allows integration with external databases and services to enable background checks of identities. This includes databases provided by government or commercial organisations including but not limited to:

- Interpol for lost or stolen passports
- International Sanction lists
- National Security Databases
- KYC/AML Databases (e.g RDC or WorldCheck)

4.4. Integration

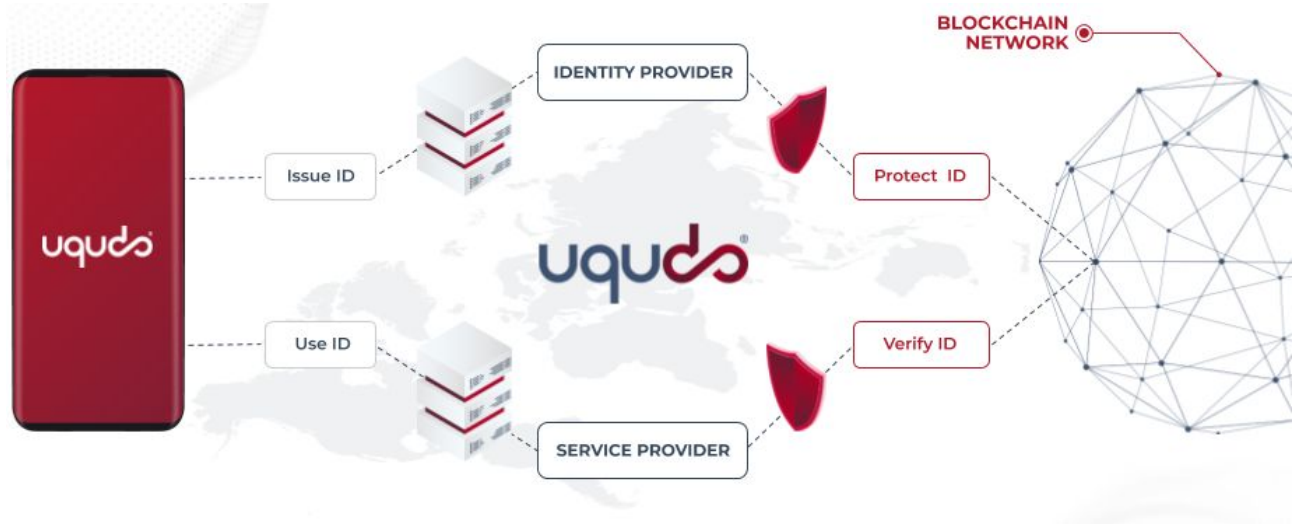
The uqudo platform provides capabilities to store the onboarded personal data into the backend of your organisation. It is also possible to share the data with third parties such as affiliates with the consent of the user.

Identity Wallet & Blockchain

uqudo has developed a unique way to store collected IDs in an ID digital wallet. The wallet manages data stored on the phone and complies with GDPR and strict data privacy laws. It enables the user to take control of their data and share it with consent. The wallet will enable the ease of integration with other organisations that either store, process or transmit the identity.

The platform has capitalised on the blockchain data and this feature can be enabled to provide an extra layer of security and enable more rich use cases around data sharing and consent. The ID wallet is integrated with permissioned and public ledgers. No data is stored in the blockchain and the solution is compatible with the data privacy and GDPR.

uqudo platform only stores hashes and public keys on the blockchain. It ensures compliance with data privacy regulations while protecting the integrity of the shared data. The uqudo platform is blockchain agnostic and works with both private and public blockchain. The platform currently supports Hyperledger Fabric, Quorum and Ethereum. Other blockchain platforms are possible if required.



The illustration above gives an overview of the technical implementations. There are three factors:

- Identity Provider
- Service Provider
- ID Wallet on the mobile device of the user

A user can have multiple identities from different Identity Providers. Identity Providers verify the identity of users during enrolment (e.g. through offline or online verification processes). They store the attributes collected during the enrolment on their databases. Users can use the mobile app to load the attributes from any Identity Provider. The Identity Provider combines the attributes (claims) in a package called ID Card. It is possible to issue multiple ID Cards for the same user with different attributes. During the issuing process, the Identity Provider calculates the hashes for the issued ID Card and stores it on the blockchain.

A user can use the ID Cards on his mobile app to authenticate or register with Service Providers (SP). Service Providers can define which ID Card they accept. The Service Provider receives the ID Card from the mobile app and verifies the attributes with the block chain ensuring the attributes are genuine and issued by the Identity Provider.

APIs

The uqudo platform does not store personal data. After verification, the data is passed to the backend of your organisation. The uqudo platform supports standard protocols for the integration including:

- REST APIs to integrate with your backend
- Datastore APIs such as LDAP or SQL
- Federation APIs such as OAuth, OpenID Connect or SAML

4.5. Access

Passwordless
Once a user is onboarded, authentication ensures the identity of a user each time the user interacts with your organisation.

The uqudo platform provides passwordless authentication through biometrics based on FIDO Standards. One of the key characteristics of FIDO is to provide an Omni-channel experience for end users which is frictionless, secure and respects privacy principles. It is fairly simple for your organisation to implement and adapt to new modalities of authentication without the need for re-engineering therefore ensuring operating costs are low.

Benefits of verifying with FIDO standards include:

- Interoperable approach
- Privacy-preserving
- Protection from phishing/man-in-the-middle (MITM) attacks
- Reduction of complexity and costs
- A global standard endorsed by government regulations worldwide
- Certification program for compliance
- Major industry players are committed

The platform allows for multiple use cases beyond traditional multi-factor authentication (MFA). Further examples where the access layer of the platform could be implemented include:

- Kiosks
- Smart speakers and Home Assistants
- ATMs
- Authentication of IoT devices
- Smart devices such as wearables
- RCS channels – authentication of communication with chatbots
- Call Centres

The FIDO protocols are designed from the ground up to protect user privacy. The protocols do not provide information that can be used by different online services to collaborate and track a user across services. Biometric information never leaves the user's device.

Account Recovery
If users need to recover their account (e.g. after device reset) they can easily do so without calling the service line or entering security questions. The requirement is to perform another face authentication which will be compared to the picture captured during the initial onboarding.

Behaviour Biometrics
The uqudo platform can use behavioural biometrics to verify and authenticate an individual user in real-time. An algorithm measures and records how the users use their devices. The uqudo platform uses scores to represent the certainty of the user's identity.