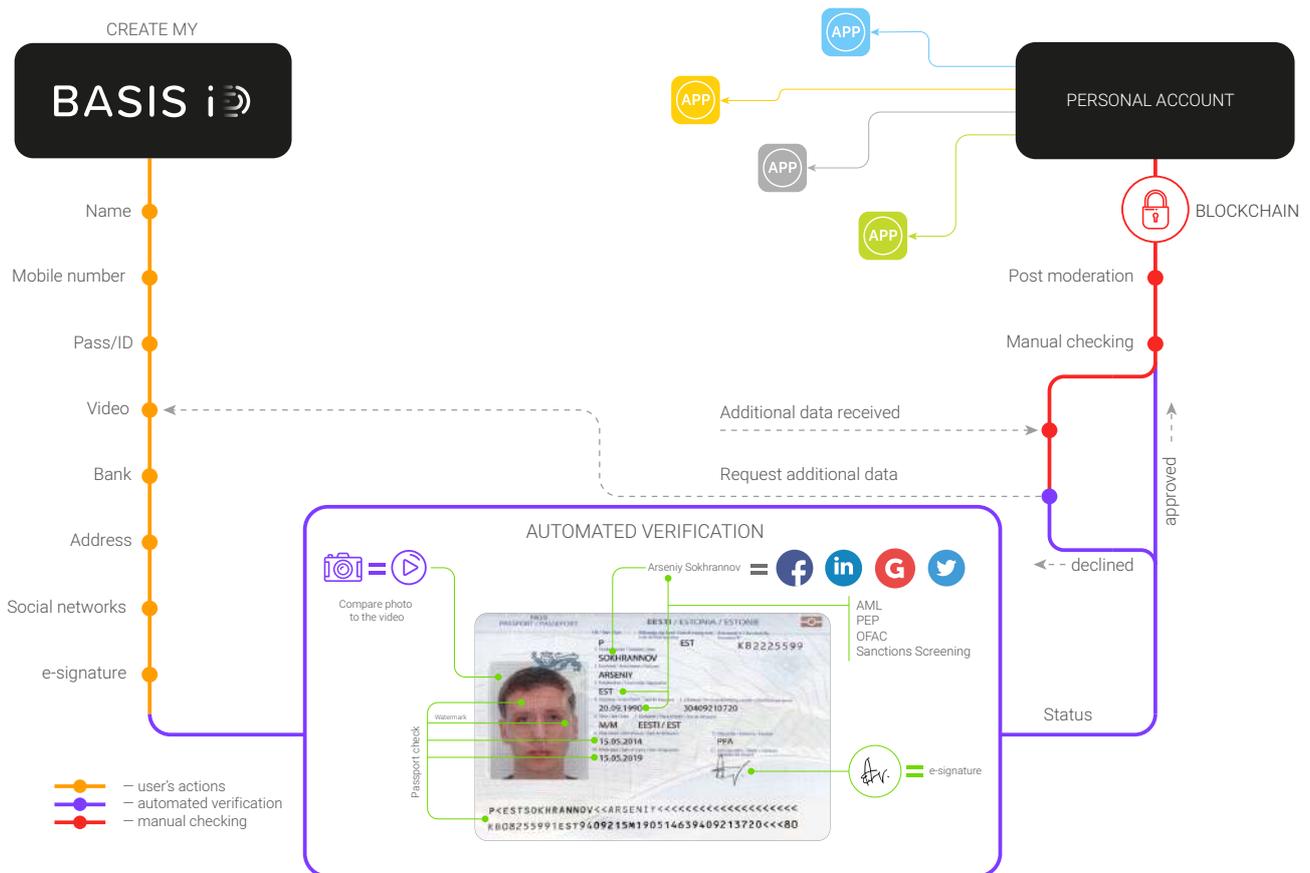


BASIS iD

# BASIS ID

Functionality Document

BASIS ID's objective is to provide their clients a secure and systematic way of verifying their potential customers' identities. With this in mind, BASIS ID offers a variety of options – some of which are optional – that BASIS ID's clients can use to maximize their customer base's legitimacy and security.



How BASIS ID works: get onboarded by BASIS ID in 8 simple steps



**1**

Check your identity

Basic personal information: name, gender, birthday and nationality



**2**

Phone number validation

OTP message is sent to the customer



**3**

Scan your passport or ID card

Document is authenticated against security features



**4**

Record a video

Biometric facial recognition ensures the person is actually present



**5**

Debit card validation

Information about bank that verified your user before



**6**

Address validation

Scan utility bill or receive a verification code by mail



**7**

Sign an agreement

Electronic signature is following ESIGN, UETA and eIDAS standards



**8**

Sanctions screening

Global coverage for AML, PEP, OFAC and Sanctions Screening

# 1

## Verification of end-customer's full name, including any aliases

The system contains the following end-customer's details:

- Name
- Surname
- Date of Birth
- Gender
- Country of Citizenship

These details are obtained from the questionnaire which is provided by clients to the end-customers. From there, these details are compared with the details that are found in either the machine readable passport (MRP or travel document) or the ID card with machine readable zone (MRZ) – both of which follow the ICAO standards.

---

### **Machine readable passport (MRP)**

MRP is a machine-readable travel document (MRTD) with data on the identity page encoded in optical character recognition format.

### **Machine Readable Zone (MRZ)**

MRZ is a form of data that is filled with 44 characters that is stuffed in two lines. It is usually found at the bottom of an identity page.

### **ICAO standards**

The ICAO Document 9303 describes three types of document formats. The passport booklets are usually issued in a "Type 3" format while the identity cards and passport cards fall under the "Type 1" category. The MRZ of a "Type 3" travel document spans two and each line is 44 characters long. The following information must be provided in the zone: Name; Passport Number; Nationality; Date of birth; Sex.

## 2

### Verification of end-customer's phone number (optional)

BASIS ID will send the end-customer an OTP code through a SMS via the Nexmo platform. The end-customer will have to key in the OTP code as shown in the SMS into the website to confirm that he is the person whom the phone number in the website matches with. Upon confirmation, the "Confirmed" status will appear in the client's CRM dashboard under the end-user profile.

## 3

### Verification of end-customer's identity via documents

These are the types of identification that BASIS ID accepts as identity documents:

- Passports
- ID cards
- National ID cards/ CPRs.

BASIS ID checks these documents for any signs of tampering which could indicate a possibility of fraud/ misuse of the documents. This is accomplished by the four following analysis tools:

- Average Distance of Neighbor Pixels Algorithm
- Error Level Analysis
- Luminance Gradient
- Copy-move detection

**Average-Distance of Neighbor Pixels Algorithm**

Anomalies in the color of neighboring pixels will be highlighted. Unusual colors will stand out as bright white and reveals that there is a high chance that the image was modified.

**Error Level Analysis**

A picture that is unlikely to be tampered with should have all the objects in the picture to be at a roughly similar coloring. Otherwise, if anything stands out as bright white, then it indicates that it last thing modified since it is at a higher potential error level than the rest of the image. In other words, bright white spots reveal that the objects have been enhanced digitally.

**Luminance Gradient**

This tool is effective in identifying any signs of digital manipulation like Blur, Chroma Key, Liquify and Retouch in the photo. The entire image on luminance gradient should contain bumpy noise and jagged lines. Otherwise, a digitally manipulated image will show smooth blurs or straight edges.

Additionally, a genuine photo should have similar lighting in all of its surface.

**Copy-move detection**

This tool is useful in spotting any signs of “copy-paste”, clone stamp, extrusion and healing brush in the photo. Because the color-move detection analyses color schemes, colors that are not “in the right place” will be revealed and highlighted for the client’s reference. Highly-lighted spots could signify that color correction or insertion had taken place.

# 4

## Verification of end-customer's identity via video recording

### Recording Process:

The client has to provide sufficient video-capturing capabilities that can record at least 10 seconds worth of videos of their end-customers' faces or, faces with the necessary documents like passports and national identity cards.

The video can be captured by any of the following:

- Mobile Application
- Web Interface
- Self-checkout machines with camera
- Camera on the POS terminal
- Any other hardware device using the software that is integrated with BASIS ID APIs.

Subsequently, the video will be transferred to BASIS ID's servers for back-end biometric facial recognition and motion capture validation.

### Verification Process:

The system will check if the end-customer had edited the photo with third-party applications (like Photoshop or Illustrator), except in cases when the photo has been edited, printed and provided for verification.

In addition to verifying the legitimacy of the video provided, there are four layers of verification that the client will benefit from.

### Automated Verification:

System cuts 22 frames with the end-customer's face and compares these frames with the photo in the passport/ID card. At

the same time, the system will examine the end-customer's movement on the video to ensure that there are no signs of fraud carried out in the video recording.

From there, the system will specify a status out of the two statuses, which is determined by a criterion. A "Confirmed" status will appear if less than 80% of the frames matches the photo in the passport/ID card. Meanwhile, should more than 80% of the frames match the photo in the passport/ID card, a "Not Confirmed" status will appear.

Manual Verification:

Customer Service agents will go through the statuses that were created by the system and verify the documents manually. There will be five agents who will verify the same end-customer's profile simultaneously. If four out of five agents decide that the details in the end-customer's profile are authentic and the faces are similar, the system administrator will approve the customer.

Otherwise, the system administrator sends a request to the end-customer to re-upload the necessary documents/information. An e-mail and a SMS with guidelines to re-upload the necessary information will be sent to the end-customer automatically.

Post-moderation:

The client may want to make a final decision on the approval of a customer after the automated and manual verification processes. In this case, the client should follow its internal verification procedures and take full responsibility over its decision to approve the end-customer.

Authorities' Verification:

The client may want external authorities and statutory bodies (e.g. Central Bank) to intervene to assist them with the verification process. In this case, BASIS ID will grant (per request) these external authorities and statutory bodies access to a special dashboard, which will create transparency between the client and authorities.

# 5

## Verification of end-customer's address against bank statements

The system uses an optical character recognition algorithm to extract the address from the photo of the bank statement. With this information, BASIS ID will use the bank's database and verification process; if they had verified the end-customer in the bank branch before; to confirm the end-customer's identification. Upon confirmation, the address verification status will be updated in the client's CRM dashboard (under end-user profile) in real time.

Any bank statement which publication date is more than three months away from the time of BASIS ID's assessment will not be accepted.

# 6

## Verification of end-customer's residential address via post mail

BASIS ID will send a physical letter that contains a unique code to the end-customer's provided address via express delivery. It will be hand delivered by a deliveryman/postman from the post office or whichever agency provides postal services.

Upon courier delivery, the end-customer will have to key in the unique code that is written in the letter into the website link that is provided in the letter. If successful, the address verification status will update in real time in the client's CRM dashboard (under end-user profile).

BASIS ID also taps onto the following to verify the physical address:

- Google Map Enterprise
- Experian Data Quality
- SmartyStreets by USPS
- Local post office branches via APIs

# 7

## Verification of business registration/ incorporation number

In a situation where the end-customer happens to be under the non-natural end-customer category, BASIS ID provides its clients the option to check that end-customer's business registration/incorporation number. Upon completion of the check, the system will return either a "Registered" or "Liquidated" status.

However, in this case, the verification process depends on the quality of BASIS ID's connections to the registries. While some countries provide BASIS ID direct access to the APIs, there are other countries which require BASIS ID to manually extract the data from the registry portal.

For this reason, the prices for corporate verification of deeper positions like directors, shareholders and UBOs will vary. Due to the prices' complexity of different registries, BASIS ID will decide on the prices on a case-by-case basis<sup>1</sup>.

---

<sup>1</sup> Details of estimated time taken for each country are revealed in the FAQ

# 8

## AML/ OFAC/ PEP/ Sanctions Screening

The screening of the end-customer will be based on the Thomson Reuters, Dow Jones, LexisNexis, and BOC blacklists provided by the client.

---

Note: BASIS ID strongly recommends that the client uses a team of experienced and qualified developers to install BASIS ID's APIs and widgets. The client should strictly follow the instructions in BASIS ID's API documentations to minimize any disruption to the onboarding process.

---

## FAQ

1. (a) What system/tool does BASIS ID use for checking the MRZ?

BASIS ID uses its own developed system which is robust in the KYC market with a validation rate of 98%.

(b) How does BASIS ID check national IDs from various countries?

A customized verification engine is created for each country's national ID. It based on the following technologies:

- Python image processing tools (BSD/MIT license)
- Custom machine readable zone coding
- Google tensorflow models
- Kaggle (for machine learning)
- Google tesseract (for text validation)

(c) What system/tool does BASIS ID use for verifying corporate information validation?

BASIS ID does not use any external providers for corporate information verification. Instead, it directly integrates with registries.

2. What are the analysis tools used to verify whether the documents have been tampered with?

#### **Average-Distance of Neighbor Pixels Algorithm**

Anomalies in the color of neighboring pixels will be highlighted. Unusual colors will stand out as bright white and reveals that there is a high chance that the image was modified.

#### **Error Level Analysis**

A picture that is unlikely to be tampered with should have all the objects in the picture to be at a roughly similar coloring. Otherwise, if anything stands out as bright white, then it indicates that it last thing modified since it is at a higher potential error level than the rest of the image. In other words, bright white spots reveal that the objects have been enhanced digitally.

#### **Luminance Gradient**

This tool is effective in identifying any signs of digital manipulation like Blur, Chroma Key, Liquify and Retouch in the photo. The entire image on luminance gradient should contain bumpy noise and jagged lines. Otherwise, a digitally manipulated image will show smooth blurs or straight edges.

Additionally, a genuine photo should have similar lighting in all of its surface.

#### **Copy-move detection**

This tool is useful in spotting any signs of “copy-paste”, clone stamp, extrusion and healing brush in the photo. Because the

color-move detection analyses color schemes, colors that are not “in the right place” will be revealed and highlighted for the client’s reference. Highly-lighted spots could signify that color correction or insertion had taken place.

3. If verification is done by the system application, will there be any further verification made by the staff in some circumstances?

Yes. The automated and manual verification processes are mandatory and done by default.

4. What is the time estimated for BASIS ID to retrieve data from each country?

BASIS ID estimates that the time taken to verify the existence of the company via corporate name and corporate registration number in Singapore to be within a maximum of 1 hour.

Meanwhile, in East Asia countries (e.g. China, Hong Kong, South Korea etc.), South-East Asian countries (e.g. Malaysia, Indonesia, Philippines, Thailand, Vietnam, etc.) and Arab countries (e.g. Bahrain, South Arabia, Qatar, Kuwait, UAE, etc.) and 200+ countries, BASIS ID estimates the response time to be up to 15 minutes.

5. Does BASIS ID also provide verification tools for email addresses and social media accounts?

Yes. These verification tools are optional. The client can inform BASIS ID if they wish to include such verification tools in their on-boarding process.

Confirmation of e-mail address:

BASIS ID sends an automatic email with a unique link inside. The end-customer is to click on the link to confirm his email address.

Similar to the OTP code system mentioned earlier, the confirmation status will appear in the clients' CRM dashboards (under end-user profile).

Confirmation of social network accounts:

The end-customer can connect his/her social media accounts to his/her BASIS ID profile. The system will then compare the name and the surname of the social media profile with the name and the surname provided in the questionnaire as well as his/her passport or ID card.