BASIS ID

AML Compliance policy

Digital era calls for new regulations which are, at times, strict and quite resourceful. BASIS ID acknowledges the struggle of SMEs that want to direct its strength and time solely on the offered services. Throughout its operation on the market, BASIS ID has developed a reliable ecosystem where complex issue of data circulation and management is made easy. BASIS ID offers a trustworthy method of authentication and verification of end-users, as well as maintaining and configuring their data. Our goal is to make the life of our clients easier, saving their time, energy and human resource on compliance matters. BASIS ID solution is compliant with data protection, Anti-Money Laundering (AML) and Counter Terrorism Financing (CTF) regulations for various market operators like FinTechs and RegTechs.

As obliged parties, our clients must identify, before any kind of transactions made, the persons carrying out the transactions or the persons on behalf of whom the transactions are conducted. BASIS ID has developed the set of semi-automated tools to perform Customer Due Diligence (CDD). The tools used focus on principles of machine learning and risk assessment, enabling to measure the potential risks of criminal activity and possibility of suspicious transactions. For AML and CTF purposes as well as to protect our clients from such circumstances, BASIS ID arranges and maintains adequate and strong measures in relation to collection, screening, monitoring and retention of data subject's data.

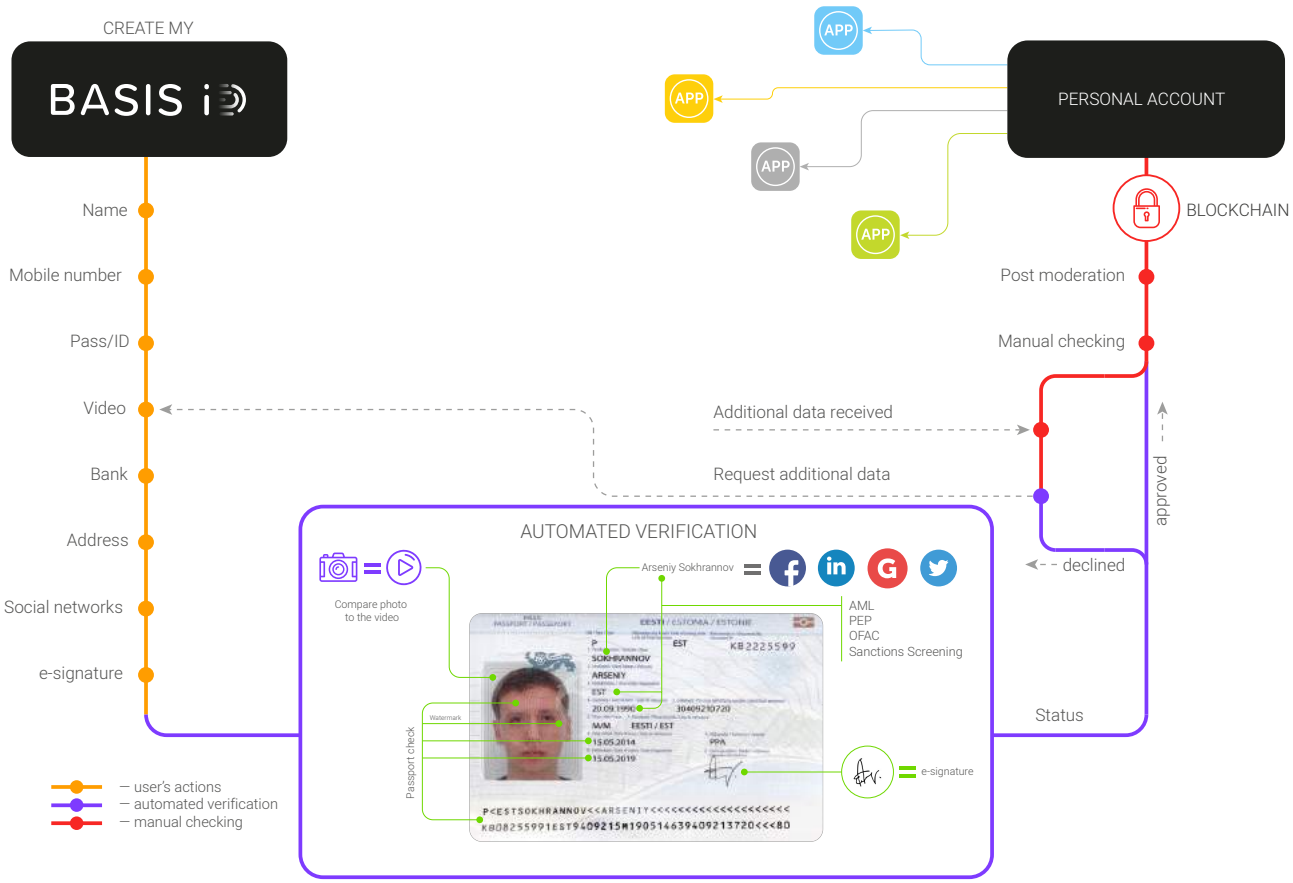
This document will represent how BASIS ID implements Know Your Customer (KYC) and CDD framework as well as how AML policy is integrated in BASIS ID services.

BASIS ID Compliance Team

Customer’s data journey

Customer enters BASIS ID verification page or BASIS ID integrated API and begins with the procedure of verification. Our user-friendly system leads the customer through the process by advising on each step of it. After the client has uploaded all the necessary information, BASIS ID proceeds with the rule-based system of analysing and checking personal information received.

The typical customer's data journey can be illustrated in the following way:



1

Identity check

BASIS ID checks data-subject's basic personal information: name, gender, birthday and nationality

2

Phone number validation

OTP message is sent to the data-subject

3

Passport/ID Card scan

Document is verified against security features

4

Video recording

Biometric facial recognition feature ensures the person is actually present

5

Debit card validation

Matching identity of the person and the payer; validating source of funds

6

Address validation

Scanning utility bill or bank statement

7

Agreement signing

Electronic signature is following ESIGN, UETA and eIDAS standards

8

Sanctions screening

Compliance with AML requirements by screening through sanctions lists

1

Verification of data-subject's full name, including any aliases

BASIS ID system collects the following data-subject's details:

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

These details are obtained from the questionnaire which is based the needs of the client. 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. BASIS ID uses its own developed system which is robust in the KYC market with a validation rate of 98%.

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 data subject's phone number

On the request of the client, BASIS ID will send the data subject an OTP code through a SMS via the Nexmo platform. The data subject will receive the 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 status "Confirmed" will appear in the client's CRM dashboard under the data subject's profile.

3 Verification of data subject's identity via documents

BASIS ID system which is build on machine learning, identifies the following documents of the data-subject:

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

The system identifies document of more than 200 countries. 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

A customised 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)

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 data subject's identity via video recording

BASIS ID system requires customers to record a video of their face from different angles.
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.

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 data subject 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 data subject'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 more than 80% of the frames matches the photo in the passport/ID card. Meanwhile, if less than 80% of the frames match the photo in the passport/ID card, a “Not Confirmed” status will be indicated.

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 data subject’s profile are authentic and the faces are similar, the system administrator will confirm the verification.

Otherwise, the system administrator sends a request to the data subject 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 data subject'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 data subject's residential address

In order for clients to be compliant with AML regulations, the system asks end-users to fill in their address details and to upload (or take a picture) of their proof of address (which can be found in bank statements, utility bills or others). Then, BASIS ID verifies this information manually using trusted sources.

Alternatively, BASIS ID can verify data subject's address by sending a physical letter that contains a unique code to 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 delivery, the data subject 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 data subject's 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 legal entity, 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.

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.

AML-compliance + custom blacklists – to check users' data for correctness and trustworthiness, BASIS ID system uses acknowledged AML-service providers which cover more than 190 countries. On request of our client, we perform the check against sanctions list including, but not limited to OFAC, PEP, UN, EU, HMT. Furthermore, we have custom blacklists from governmental agencies across SouthEast Asia.

9 Internal safeguards

Apart from the tools included in our rule based and monitoring system, BASIS ID implements internal safeguards to maintain the standards of good practice.

To ensure staff professionalism and appropriate level of training, BASIS ID developed its own training programme. It includes introducing an employee to all the policies, procedures, requirements and platforms. BASIS ID personnel is trained and competent and each of the team members is subject to the duty of confidence. Before employing, BASIS ID performs background check and monitors it at the time of employment.

BASIS ID Legal Department keeps company's policies up-to-date constantly monitoring recent regulation changes and applicable case law to perform compliant services. Legal Department includes AML Compliance Team which is fully responsible for BASIS ID AML and CTF compliance and strategy. AML Compliance Officers ensure proper AML records documentation and perform audits of the whole system and the procedure reporting directly to the Board. AML Compliance Team handles suspicious activity notifications, helping BASIS ID clients to report to FIU.

10

External assessment

BASIS ID technologies are currently being audited by "Big 4" from Singapore. The audit is focusing on assessment of customers' onboarding procedure, controlling identification and verification modules, as well as the overall performance of Customer Due Diligence module. Compliance is the first priority matter for BASIS ID, this is why we are always up to date with increasing complexity of data protection or privacy regulations. The purpose of this audit is to assess BASIS ID's operating processes with respect to its functionality, reliability and safety, to detect and eliminate any potential vulnerabilities. Evaluation is based on Singapore's regulation and fuels advancement by demonstrating the accomplishments and highlighting the new plans.