Anti-Money-Laundering Features
Crypto Application Server (CAS) software

Last Update: August 2021
support@generalbytes.com

GENERAL BYTES

The CAS software for our Cryptocurrency ATMs is designed to successfully fight money laundering. The Operator (owner and operator of Cryptocurrency ATMs) can choose between a wide range of features to comply with local KYC & AML regulations. If a customer of the Operator wishes to buy or sell a Cryptocurrency, several interconnected mechanisms will work to ensure compliance with their established AML Policy. The following pages describe which mechanisms are available to the respective Operator.

TeleSign Integration

We integrate CAS with the global leader for phone identity check: TeleSign. Transactions can be restricted to customers with a "known" phone identity. When enabled by the Operator, any customer entering a phone number will have the number checked against the list maintained by the telecom provider. The provider will reveal the type of phone number used. This technique can mitigate certain fraud tactics.

Rejecting PEPs

In financial regulation, a politically exposed person (PEP) is one who has been entrusted with a prominent public function. A PEP generally presents a higher risk for potential involvement in bribery and corruption by virtue of their position and the influence that they may hold. The option Rejecting PEP's can be easily activated in the CAS.

OFAC Scan

During an identity approval process (see below: Identity Management) a manual check against the OFAC Sanctions List can be made with one click. Depending on the result (false or positive), the Operator may move the identity status to Rejected or Registered.

EU Sanction List

During identity approval (see below), an Operator can compare an Identity against the EU Sanctions List with a single click. The Operator may move the identity status to Rejected or Registered depending on the result (false or positive).

CipherTrace (3rd party service)

Transaction scoring is used to protect Operators' customers from scams and funding criminal enterprises. High risk wallet addresses (as defined by CipherTrace) are rejected when presented as a target wallet (BUY), and incoming coins (SELL) will not be automatically enabled for cash withdrawal.

ChainAnalysis (3rd party service)

ChainAnalysis KYT (Know Your Transaction) detects many patterns of risky activity, from darknet markets and scams to sanctioned addresses and anomalous transactions. Covers 90% of all cryptocurrency activity. Use the real-time KYT API to prevent withdrawals to blacklisted addresses and freeze deposits from hacks, scams, and ransomware.

Limits

The Operator may set a variety of generic limits for their customers. Identity limits for individual customers restrict individual transaction amounts on a granular level:

- Cash Limit Per Transaction
- Cash Limit Per Hour
- Cash Limit Per Day
- Cash Limit Per Week
- Cash Limit Per Month
- Cash Limit Per 3 Months
- Cash Limit Per 12 Months
- Cash Limit Per Calendar Year Quarter
- Cash Limit Per Calendar Year
- Cash Limit Per Day And Crypto Address
- Total Cash Limit Per Crypto Address

Also, machine limits may be imposed that restrict location amounts, not just the Identity - preventing mule operations at specific locations.

Manual approval

The Operator may enable special manual approval if any transaction is above “X” USD. For example, if the limit is set to 1000 USD and a customer would like to make a transaction for 1000 USD, this transaction will need to be specifically approved by the Operator.

KYC: Validation methods

To comply with local KYC demands, the Operator may request and/or require several pieces of customer information. We support the following validation methods:

- Cell Phone Number
- Selfie
- Social Security Number
- ID Card Scan Both Sides
- ID Card Scan One Side Only
- Two Documents
- Fingerprint
- Email
- Name
- Custom Field
- Third-party validation (see: *External Registration and Onfido*)

External Registration

Our AML/KYC settings include an optional integrated “External Registration Only” which enables an Operator to use its own (or bank mandated) AML/KYC 3rd party service for automated customer approval.

Onfido (3rd party service)

Onfido allows you to automate the onboarding process of new clients using AI and their team of identity experts and saving you time. In some cases, the time required to onboard new clients can be reduced from several hours to less than a minute, smoothing the user experience and increasing the security of your ATM network. In addition to these benefits, **third-party verification is sometimes a requirement by regulators in your operating jurisdiction.**

Identity Management (customers of the Operator)

Identities must be processed, reviewed, and approved to meet AML/KYC requirements. Multiple levels are available to comply with regional regulations.

● Awaiting Registration ○ The Identity has requested a transaction that requires registration. They have submitted the requested information to you. You must now review their submission, verify its authenticity, and decide whether to grant the Identity permission to continue with the requested transaction.
● Registered ○ This Identity has been reviewed and completely approved.
● Rejected ○ This Identity has been rejected for all transactions requiring registration.
● Not Registered ○ This Identity may still be permitted to conduct minimal transactions that don’t exceed certain limits and don’t require AML/KYC registration.

Upon document expiration, the system may automatically demote an Identity to “Not Registered” - forcing a KYC review & reapproval.

Notifications

Operators are able to configure notifications that enable instantaneous notification of transactions exceeding set limits. This enables the Operator to view anomalous transaction behavior within their network.

A fleet of Identity Approvers (or a mere individual) may be permitted restricted access to approve & authorize customers upon demand 24x7.

Face Capture

Operators may choose to silently capture a picture taken by the machine during a transaction. These pictures are attached to the Identity history as identity confirmation for each transaction.

Blacklists

The Operator has the option to add blacklisted wallet addresses in addition to the large list provided free with our software.

Banknote Validation

Presentation of fraudulent or counterfeit banknotes is eliminated using state-of-the-art validation techniques embedded in every machine.

Operation Hours

The Operator can set a separate opening time for each ATM. No transactions are possible outside business hours.