Positronic

Know Your Customer

VERIFY USER IDENTITY WITH PHOTO ID DOCUMENTS AND BIOMETRIC LIVENESS BINDING TO MATCH FACE-TO-PHOTO.

- Streamline the KYC process for new and returning customers
- Optical Character Recognition (OCR) and Machine Learning (AI) technology
- Biometric face-to-photo matching for liveness matching
- Mobile centric eKYC with the customer in full control of their identity information
- Document Validation Service (DVS) against government records
- Support for adjudication step where DVS is not available

Know Your Customer (eKYC) by capturing identity information from photo ID documents (such as driver's licenses, passports and ID cards) with liveness binding through biometric face-to-photo matching. The customer controls their identity by authorising release and confirmation of their identity information. Identity documents are validated through an adjudication step or through automated validation against government records through a Document Validation Service.

Capture **Match** **Adjudicate**

Capture and streamline the process for collecting new customer identity information. New customers scan their ID documents using the Positronic mobile app which utilises Optical Character Recognition (OCR) and machine learning (ML) technology to capture identity information such as name, date of birth, address and photo ID from driver's license, passport and national ID cards.

KYC

AML

Match face-to-photo ID for a 'liveness' test validation as proof to ensure that the scanned ID documents belong to the new customer. Face-to-photo matching is done through the Positronic mobile app which utilises biometric technology and Artificial Intelligence to determine liveness.

Unbanked

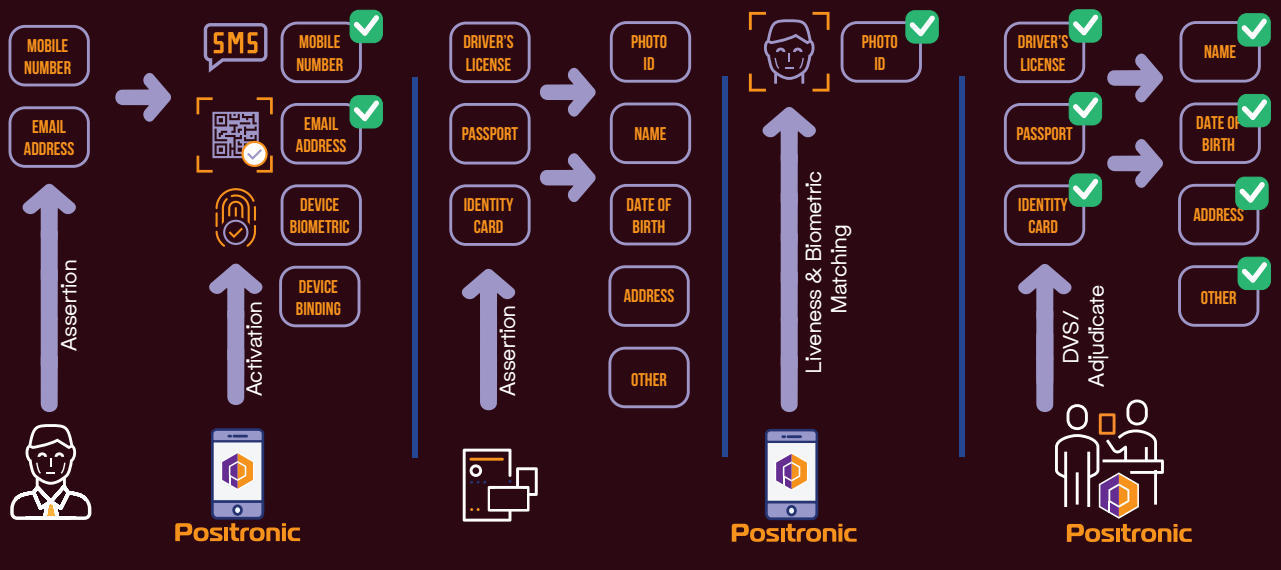
Fintech

Online Banking

Cyber ID

Adjudicate the validity and associated level of trust in the captured ID documents through existing processes including DVS validation against government records.
Adjudication and sponsored DVS activities can be conducted after ID capture as needed based on the required increased level of trust in the identity information beyond machine verified capture and liveness matching.

Identity Attributes & Trust Verification



What Can Positronic Do?

AML

Meet Anti-Money Laundering (AML) regulatory compliance requirements through the use of Positronic eKYC for collection and verification of customer identity information across digital and in-person channels. Validate ID documents against government records and in-person through existing processes for adjudication of the customer identity.

Fintech

Enable FinTechs to re-use and leverage the Positronic eKYC pre-verified customer identity information that has been captured and validated by another entity.
Customers remain in control of their verified identity information through ongoing use of Positronic to give consent for the release of their identity information

Cyber ID

White label and operate Positronic as a Cyber ID Scheme to enable customer identification and onboarding for businesses seeking eKYC and AML compliance. Provide a convenient pre-verified portable cyber identity mobile token that is in full control of the customer through active consent-based release of identity information.

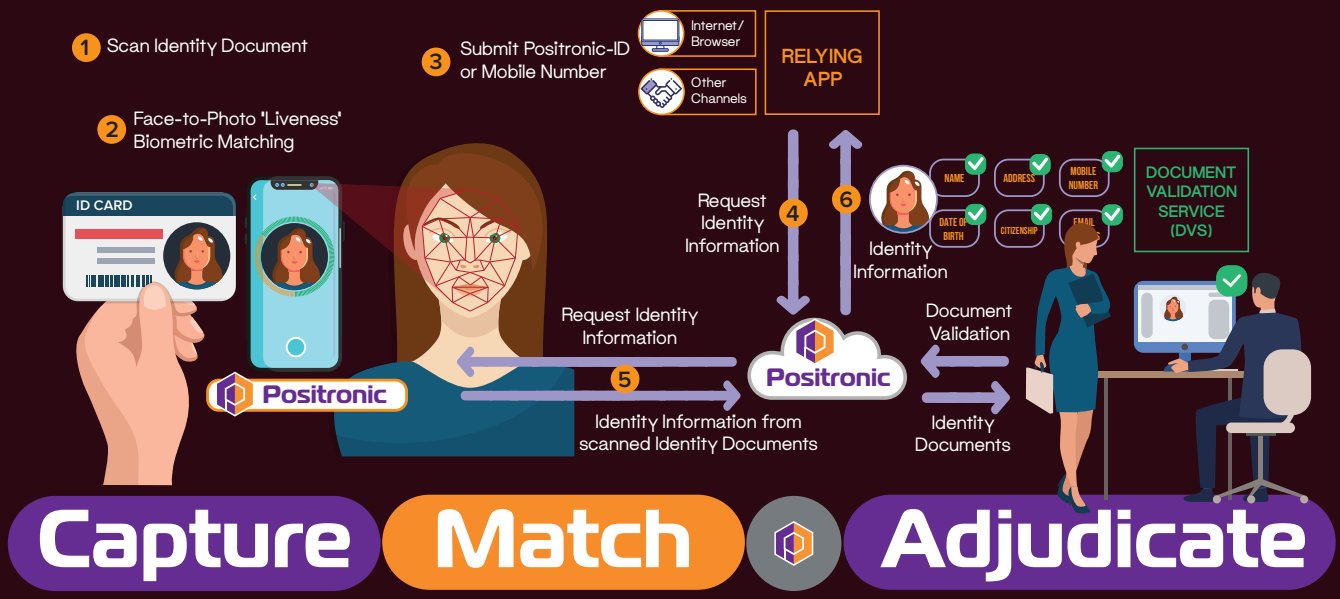
Online Banking

Ongoing use of Positronic as an authentication token for Online Banking to enable strong Multi-Factor Authentication of the customer for Login Access Control and Transaction Verification across all digital channels (such as Internet Banking, Tele-Banking, IVR, Chatbots, Mobile Banking, POS, ATM) through an independent channel for authentication.

Unbanked

Reach out to geographically dispersed populations of Unbanked users where in-person face-to-face KYC onboarding is not viable. Positronic KYC enables a fully digital solution for onboarding unbanked users by electronically capturing identity documents, biometric matching the photo ID and supporting existing adjudication processes where the user is interviewed through videotelephony.

How Does Positronic Work?



1. The user installs the Positronic app on their mobile phone and scans their identity documents using the phone's camera. The Positronic app uses OCR and ML technology to capture identity information such as name, date of birth, address and photo from the identity document.

2. Positronic uses the selfie camera to complete a biometric face-to-photo match for 'live-ness' validation to ensure that the captured identity document belongs to the user.

3. The user submits their Positronic-ID reference number (or mobile number) to Relying Applications to provide their identity for KYC onboarding.

4. Relying Applications use the Positronic-ID reference number to request user identity information from the Positronic backend. The request indicates the required identity attributes, trust level and the adjudication method, i.e. electronically via DVS or manually done in-person or via videotelephony conducted by an authorised representative.

5. The request for the identity information is sent to the user's Positronic app for consent to release the information to the Relying Application; this requires the user to sign into the Positronic app (biometric or PIN); review a summary of the identity requested; and give consent to release their identity information to the backend.

6. The user's identity information and associated level of trust is returned to the Relying Application. Trust Levels are based on how the identity information has been verified; i.e. DVS, biometric matching, in-person/videotelephony adjudication, and the number of identity documents used as sources for the user's identity.

Salt Cybersecurity
Office 4, 219 Kensington High Street,
London W8 6BD, UK

UK/EU & Australia/AsiaPac
T: +44-20-3966-1686 (UK/EU)
T: +61-3-9614-4416 (AU/AsiaPac)
E: sales.uk@saltgroup.com.au