Positronic

Know Your Customer

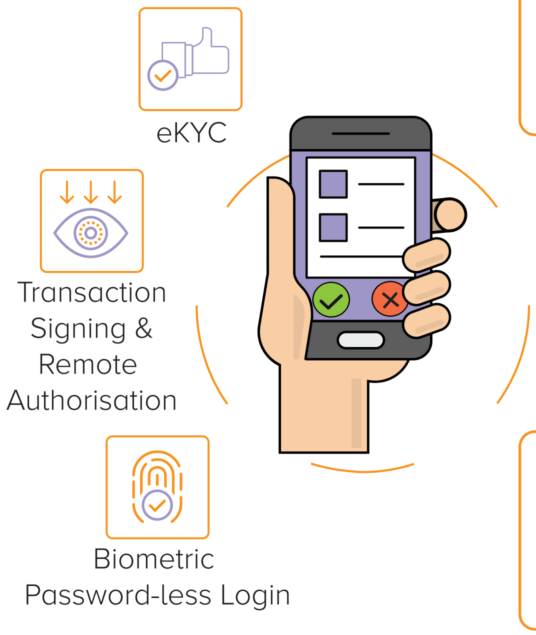
VERIFY USER IDENTITY WITH BIOMETRIC FACE-TO-PHOTO ID MATCHING THEN USE AS A MOBILE MFA SECURITY TOKEN FOR ONGOING USER & TRANSACTION AUTHENTICATION INDEPENDENT & DECOUPLED FROM THE SERVICE CHANNEL

Positronic is a contemporary mobile security token for Know Your Customer (eKYC) onboarding and an ongoing contemporary Multi-Factor Authentication (MFA) mobile token.

Positronic's eKYC capability enables electronic customer onboarding through verification of the customer's evidence-of-identity information from photo ID documents (such as driver's licenses and passports) with liveness binding through biometric face-to-photo ID matching. The customer controls their identity through Positronic's remote authorisation capability to release identity information to requesting parties. Evidence-of-Identity (EOI) documents are validated through an adjudication step or through automated validation against government records via a Document Validation Service (DVS).

Positronic's MFA capability enables ongoing use of the mobile token for authentication of the user identity during login and authentication of transactions after login. Positronic is 'connected' in that the authentication responses are returned directly to the Safetronic authentication platform thereby enabling authentication that is independent of the delivery channel that initiated the request.

What Can Positronic Do?


eKYC
Transaction Signing & Remote Authorisation
Biometric Password-less Login

Know Your Customer (**eKYC**) with evidence of identity capture and verification for **Customer Onboarding** using photoID and biometric liveness binding to match the face-to-photo ID

Multi-Factor Authenticator (MFA) for high value **Transaction Signing** with WYSIWYS (What You See Is What You Sign) and **Remote Authorisation** independent of the delivery channel that initiated the request

LOGIN

Biometric Password-less Login for strong user authentication during logon to digital channels replacing traditional username/passwords.

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.

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.

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.

KYC

Online Banking

AML

Cyber ID

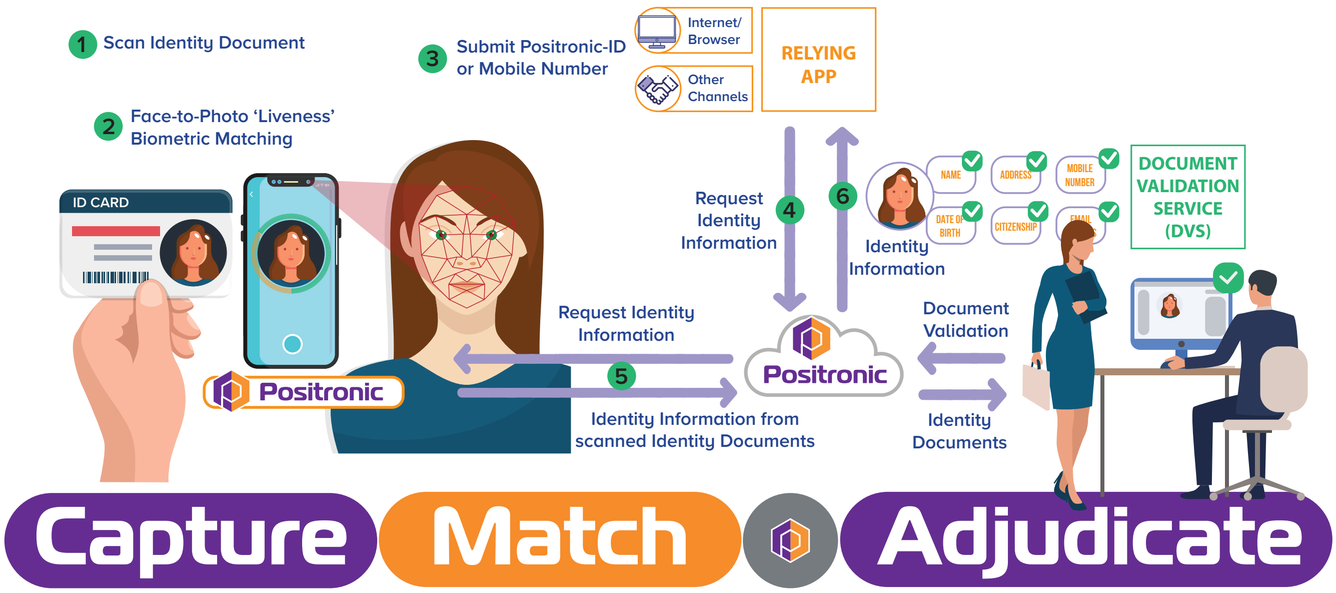
Unbanked

Fintech

Capture Match Adjudicate

How Does Positronic eKYC Work?

The diagram below outlines Positronic Know Your Customer (eKYC) for Customer Onboarding through evidence of identity capture and verification using biometric liveness binding to match the face-to-photo ID, and, adjudication through existing processes including DVS validation against government records.



1 Scan Identity Document

2 Face-to-Photo 'Liveness' Biometric Matching

3 Submit Positronic-ID or Mobile Number

Internet/ Browser

Other Channels

RELYING APP

Request Identity Information 4

6 Identity Information

DOCUMENT VALIDATION SERVICE (DVS)

Request Identity Information

5 Identity Information from scanned Identity Documents

Document Validation

Identity Documents

Capture Match Adjudicate

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 'liveness' 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.

Typical Positronic eKYC Use Cases

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 to FinTechs for rapid eKYC and service onboarding.

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

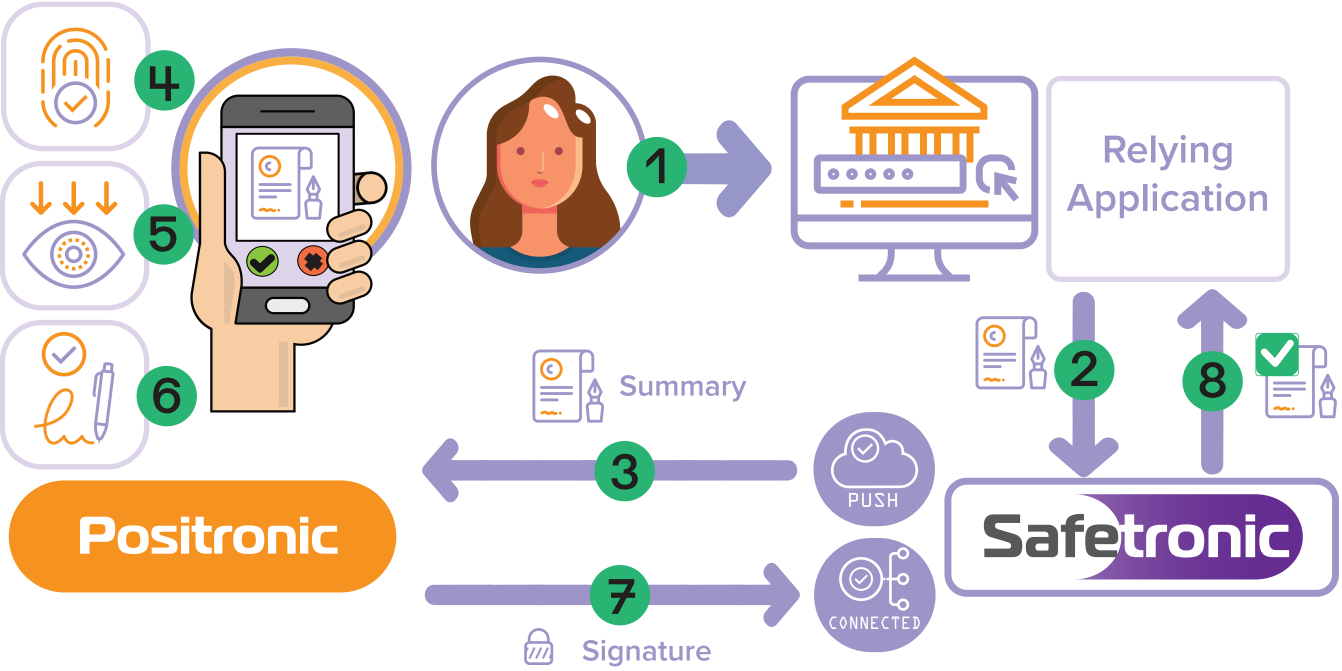
Ongoing use of Positronic as an authentication token for **Online Banking** to enable strong **Multi-Factor Authentication** of the customer for Login Access Control and Transaction Verification across all digital channels (such as Internet Banking, Tele-Banking, IVR, Chatbots, Mobile Banking, POS, ATM)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

The diagram below outlines Positronic multi-factor authentication for Transaction Signing, Password-less Biometric Login and Remote Authorisation, through an independent channel for authentication / authorisation.



1. User initiates a Transaction (or Password-less Biometric Login) or a Remote Authorisation
2. Relying Application requests multi-factor authentication for a Summary
3. Safetronic sends an Authentication Request to the User's Positronic security token
4. User Biometric (or PIN) is used to sign-in to Positronic
5. User reviews a summary of the Transaction Summary received
6. User Approves/Declines the request
7. Positronic generates a cryptographic signature of the Approval/Decline and submits the Authentication/Authorisation Signature response directly back to Safetronic (via Frontier)
8. Safetronic validates the cryptographic signature and if Transaction / Password-less Login returns the authentication response to the Relying Application. If the MFA was in response to a Remote Authorisation, Safetronic actions the Remote Authorisation (e.g. releasing eKYC identity information, signing with a Roaming Certificate)

Typical Positronic MFA Uses

- ✓ Mobile Soft Token used for 2FA Biometric Login to Internet Banking, e-Government Portals and Corporate Online Services
- ✓ High Value Transaction Signing with WYSIWYS (What You See Is What You Sign)
- ✓ Quorum Approvals and Advanced Workflows with separation of duties where the Initiator of Payment Instruction is not authorised to approve; with multiple Authorisers
- ✓ Hardware Token replacement

Benefits of Positronic

- Positronic mobile security tokens operate as a single authenticator that can be used identically across all digital services to create an independent channel for authentication whereby the authentication and remote authorisation requests and responses are direct with the user's Positronic mobile token

- Positronic mobile security tokens combine eKYC and MFA into a single security token that includes the 'step-up' customer identity verification that is typically needed before a security token is issued

- Positronic provides a cryptographically based authentication and remote authorisation service that utilises internationally recognised and approved standards for cryptographic signature generation that provide surety that the authentication/authorisation signature was generated on the registered device; and through biometric or app PIN, i.e. that the user was in charge of the device at the time of signature generation and submission to the Safetronic authentication platform

- Positronic tokens comply with contemporary standards and specifications as prescribed by NIST. This applies to the use of particular cryptographic and related algorithms, cryptographic key usage and e-Authentication assurance guidelines in respect to multi-factor authentication.

- Positronic eKYC pre-verified customer identity information can be re-used and leveraged by multiple entities. Customers remain in control of their identity information through remote authorisation to give consent for the release of their identity information.

Technical Info

- Supported on Android and iOS
- On-device cryptographic signature generation using a protected unique key
- Supports multiple methods of delivering authentication requests: Push Network, Encrypted QR Codes and Inter-App
- Biometric (Face, Fingerprint) and app PIN with central policy Biometric enforcement
- Dynamic Linking, WYSIWYS (What You See Is What You Sign)
- Strong User & Transaction Authentication: Knowledge, Possession, Inherence
- Runtime App Self-Protection (RASP) Anti-cloning and Jailbreak/Root detection
- Advanced electronic signatures uniquely linked to the signer

Salt Group Pty Ltd
Level 30, 459 Collins Street
Melbourne VIC 3000
Australia

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