THALES
Building a future we can all trust

ID verification for financial institutions

Advanced security verification
of ID documents

ID verification for financial institutions
Advanced security verification of ID documents

Verify your customers' genuine identity with frictionless ID document forensics and biometric checks, optimised for digital banking and leveraging information from more than 2000 active identity document types worldwide. Biometric checks are performed with facial recognition and liveness detection, which allows the solution to proof that the person requesting the service is a real person and owner of the document.

The consumer of today wants to handle the vast majority of their banking needs on digital and unattended channels, so that any interaction is frictionless and fast. As a result, financial institutions are consistently seeking solutions to increase their reach, engage their customers and meet them on the digital channel of their choice.

But constantly reinforced anti-money laundering (AML), countering the financing of terrorism (CFT) and know your customer (KYC) regulatory compliance and risk management considerations dictate that you must thoroughly verify the identity of customers before onboarding them as new clients, or subscribing them to a new service. Doing so manually poses a challenge, considering the huge number of identity documents you may have to check and possible human error you may face.

Our Gemalto ID verification is the answer for financial institutions looking to deploy a fast, convenient and compliant identity verification solution. It guarantees consistency across branches and self-service digital channels, and it complies with the latest AML regulations.

Our ID verification template database includes:

▌ 100% of MRZ passports in circulation

▌ 100% e-passport coverage

▌ 100% of European identity cards

▌ A worldwide coverage of passports, ID documents, driving licenses and residence permits

Our document verification module offers different service levels in accordance with the underlying document type (electronic vs non-electronic) and available document capture infrastructure deployed.

▌ ID document verification (level 1) offers a comprehensive set of visual verification actions of the integrity and consistency of the identity document. Many of them are performed over the captured document image in white-ambient light.

▌ Advanced ID document verification (level 2) using scanners can provide more verifications of the security patterns of identity documents while using 3 light spectrums (white, infra-red, ultra-violet).

ID verification service levels

As the migration to electronic identity documents continues, there is still a large number of valid non-electronic identity documents available in the industry. ID document verification provides thorough visual security verifications of the different security features in identity documents existing in the different light spectrums: white, infra-red and ultra-violet.

ID verification level 2 can be performed with high-end scanners to capture the document. It allows you to verify tens of security features, such as the existence of visual patterns and color bands, in just a few seconds. It also allows you to perform other security actions over the different light spectrums, delivering a strong visual verification of the identity document authenticity and non-forgery.

Benefits with our solution:

▌ A team of experts in identity document manufacturing designs the security checks

▌ Well established relationships with forensic labs and border control agencies

▌ Knowledge exchange with Interpol

▌ Extensive knowledge of new documents deployed in the field through our activity in identity document manufacturing

Visible security patterns verification (Level 1)

Ultra violet verification (Level 2)

An overview of the different document verification levels:

LEVEL 1 VERIFICATION

▌ Identification of document (country, type, version)

▌ Integrity verification of the document's MRZ (Machine Readable Zone)

▌ Format validation of VIZ (Visual Inspection Zone) fields in accordance with ICAO (International Civil Aviation Organization) standards

▌ MRZ vs VIZ consistency

▌ Verification of document validity (expiry date)

▌ Verification of visual security features and patterns over white-ambient light

▌ MRZ & VIZ data export

LEVEL 2 VERIFICATION

▌ All level 1 verifications

▌ Verification of visual security features present under 3 light spectrums: white, infra-red, ultra-violet

▌ Presence or absence of patterns and color band checks

▌ UV dull paper checks

▌ IR B900 ink check

▌ Photo replacement check

▌ Luminance checks

▌ Hidden images

Level 2-e (electronic) verifications option is also supported by our Gemalto ID Verification:

The solution provides additional capabilities to check the chip authenticity and non-forgery by checking the CSCA PKI (Country Signing Certificate Authority, public key infrastructure) signature of the chip with the certificates published by the issuing country of the travel document. This certificate database is constantly updated thanks to our involvement in border control and governmental identity verification solutions.

ICAO document with the following details:

▌ Verification of chip validity, through Passive Authentication (PA)

▌ Verification of non-forgery of the chip, through CSCA certificate chain validation

▌ Basic access control (BAC), and reading of demographics and portrait

▌ Extended access control (EAC), allowing reading of fingerprints

▌ Other electronic document reading on demand

▌ 3-way chip integrity validation with document visual data page (VIZ vs MRZ vs chip)

▌ Optional: match photo on chip vs document

How does it work?

The following example gives a global vision of the various verifications done on a European ID document. On this document, **up to 38 verification checks can be performed:**

▌ 28 verification checks related to data format: Does the MRZ have the expected format?

▌ 6 verification checks related to data integrity: e.g. date of birth check OCR vs. MRZ or date of expiry

▌ 4 advanced security pattern verification checks. e.g. security patterns presence check

The following list describes security verifications that can be performed on the ID document:

Optical character reading Data 1

- TD1 type field check
- Date of birth check digit test
- Primary Identifier
- TD1 number of rows and columns
- Document Type
- Secondary Identifier
- Document number check digit test
- Document expired check

Optical character reading Data 2

- OCR Document Number
- OCR Last Name
- OCR Expiry Date
- OCR Issuing Date
- Issuing State
- Date Of Birth

Data integrity checks

- Valid issuing state
- Valid Expiry date

- Valid sex field
- Valid nationality
- Valid date of birth check
- Composite check Digit
- Expiry Date check Digit
- Correct padding
- Nationality check
- MRZ Check
- VIS Identification

Visual Inspection Zone

- VIS Chip Presence Check
- VIS Optical Visual Inspection Map
- VIS Background Printing Back
- VIS Identification Back
- Specific security patterns
- Watermarks

Only with IR/UV reading:

- IR Pattern
- UV Pattern

Advanced visual security patterns verifications (level 1)

These are some examples of advanced security patterns checks provided by our ID verification solution. The verifications depend on each ID document.

The photos highlights some of the areas for which advanced security patterns are checked.

These verifications have several different natures:

- Graphical visuals
- Kineprint
- Guilloches lines on picture
- Presence of graphical visual on face picture
- Duplicated face picture in specific area
- Specific document signs & graphics (flags, shield, stamps, etc…)
- Optical variable ink
- Latent image
- Rainbow coloring
- Microprinting
- Security threads
- Metameric colors

> Thalesgroup.com <