IDEMIA
Identity Platform

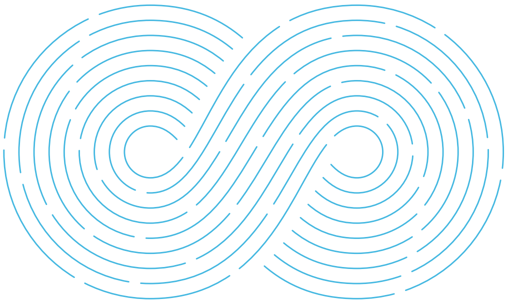
Proofing, management, and authentication, all in one

IDEMIA

We live in a world where the physical and digital converge, and where being identified digitally is becoming an integral part of our daily lives.

The IDEMIA Identity Platform is a powerful solution for enterprises and service providers to verify, manage and authenticate digital identities in a secure, trusted and convenient manner.

Contents



The need for a trusted digital identity

In a digital world where customers expect access to services anytime and anywhere and where identity theft and fraud risks are higher than ever before, the need to securely onboard and verify a customer's identity is critical for enterprises. A solution that provides a secure and seamless user experience while mitigating fraud and complying with regulations can be the key to an enterprise's success in the market.

Why digital identity?

Digital identity is the cornerstone of a complete digital experience that customers now expect. Common tasks such as enrolling for a new service, logging into an existing service, making changes to an existing account, or performing a payment all rely on customers having a digital identity and being able to prove who they are. Without a verified digital identity, companies open themselves up to fraud, regulatory penalties and exposure to other security risks.

A trusted digital identity enables parties to:

Build trust in the digital ecosystem

Digital identity is essential to establish an online model of trust that helps validate transactions and user identities reliably.

Simplify compliance and the burden of proof

Digital identity can help mobile operators, financial institutions and other service providers comply with Know-Your-Customer and Anti-Money Laundering regulations by automating and streamlining the identity verification process

Protect privacy

A well designed digital identity system only discloses the credentials that are required for each specific service, with user consent, in compliance with requirements such as the European Union's General Data Protection Regulation (GDPR), the Asian-Pacific CBPR (Cross-Border Privacy Rules) or the California Consumer Privacy Act.

Save time and costs

Digital identity has the ability to save time and money for both organizations and consumers by streamlining onboarding processes, signature of contracts and access to services.

Personalize the consumer experience

Digital identity is key to building a consistent and highly personalized consumer experience across every channel, be it online, on mobile, via a call-center, in-store, or at the doorstep.

Reduce fraud

A dynamic and multi-layered identity verification approach helps to mitigate fraud and the huge financial losses and reputational damage associated with it.

IDEMIA
Identity Platform

The IDEMIA Identity Platform enables mobile operators, financial institutions and other service providers to enroll, manage, and authenticate customers' digital identities. It enables the entire lifecycle of a digital identity from the moment that it is created, to its use by any number of parties for secure and trusted authentication, all while remaining subject to a user's consent.

IDEMIA's Identity Platform is built on a modular, API-first framework. This means that it is flexible enough to handle the varying needs of each service provider and scalable to the point that it can be integrated with legacy systems and third-party sources for a full spectrum of identity proofing, management, compliance and authentication.

IDEMIA Identity Platform functionalities

Identity Proofing	Identity Management	Identity Authentication
ID document capture & verification	ID document database storage	Two-Factor authentication (2FA)
Biometric capture & verification	Biometric database storage	Multi-Factor authentication
Root of trust checks	Data deduplication	Biometric authentication
AML/KYC compliance checks	Case management for manual adjudication	Risk-based authentication
Third-party database and verification services	ID orchestrator for workflow management	Identity federation
	Universal connector	

Key benefits

Adaptable	Proving and verifying identities is done differently around the world (multiple ID document templates, diverse regulations around the use and storage of biometric data, etc.). Since different regions and businesses are required to deal with different documents, regulations and workflows. Highly configurable, it provides the flexibility that businesses need to adapt the technology to workflows and local regulations.
Interoperable	The platform is delivered as a cloud-based service for maximum scalability and availability no matter the country or region. A single API unifies all ID verification and management processes, connecting to trusted internal or external sources. The API-driven architecture helps service providers integrate the solution within their systems. For ID document or biometric capture, IDEMIA mobile Software Development Kits (SDKs) are ready to use for easy integration into any service provider's specific mobile application.
Omnichannel	To ensure convenience and a true cross-channel experience, the platform enables customers to complete both enrollment and authentication processes from any location including in-branch, online, with a mobile app, in the field, or at a kiosk or ATM.
Modular	Depending on the business needs and use case, the platform can be broken down into separate components and scaled as the business grows.
Compliant	The platform meets the stringent and ever-changing regulatory and standards requirements for digital identity: Anti-Money Laundering (AML), Know Your Customer (KYC), watchlist exclusions (lost/stolen IDs, suspect persons, etc.) and other industry regulations including PSD2[1], GDPR[2] and eIDAS[3].
Secure	All stored documents and biometric data are held and managed by the service provider, with the highest standards of security and integrity. It ensures the privacy of data, both for companies and consumers, according to privacy regulations such as the European Union's.
Control & Consent	Enterprises can ensure that consumers retain control over their data, which cannot be used or shared without their explicit consent, and/or as permitted by law.

[1] Payment Service Directive 2

[2] General Data Protection Regulation

[3] Electronic Identification and Trust Services

Biometrics at the core

The use of biometrics combines security with convenience. It guarantees the uniqueness of a person's identity and thus ensures that the identity can be trusted. It also enables a simpler and more secure alternative to traditional methods of authentication, such as passwords and PINs.

A key underlying component of the platform is IDEMIA's biometric processing engine called MBSS (Multi-Biometric Search Services). MBSS handles any type of biometric data including face, finger, and iris.

With more than 40 years of experience, IDEMIA has the longest history of top-tier performance in biometric technology in independent tests than any other vendor on the market.

IDEMIA's fingerprint, face and iris algorithms rank amongst the top three in numerous benchmarks performed by NIST (The National Institute of Standards and Technology in the United States). They are used by intelligence agencies and police forces around the world.

These algorithms also lie at the heart of the world's largest biometric identity system in India: Aadhaar. This system has enabled the UIDAI (Unique Identification Authority of India) to provide a unique identity number to over 1.3 billion residents. Each number is linked to three biometric modalities: 10 fingerprints, 2 irises, and the face, at an average of 1 million per day.

Reaping even more benefits by becoming an Identity Provider

The IDEMIA Identity Platform enables service providers to become Identity Providers and to assume a key role in the digital ecosystem, by providing identity services to third parties:

Identity proofing

Authentication

Identity management

Banks and mobile operators are particularly well-placed to provide identity services with a high-level of assurance, notably because they:

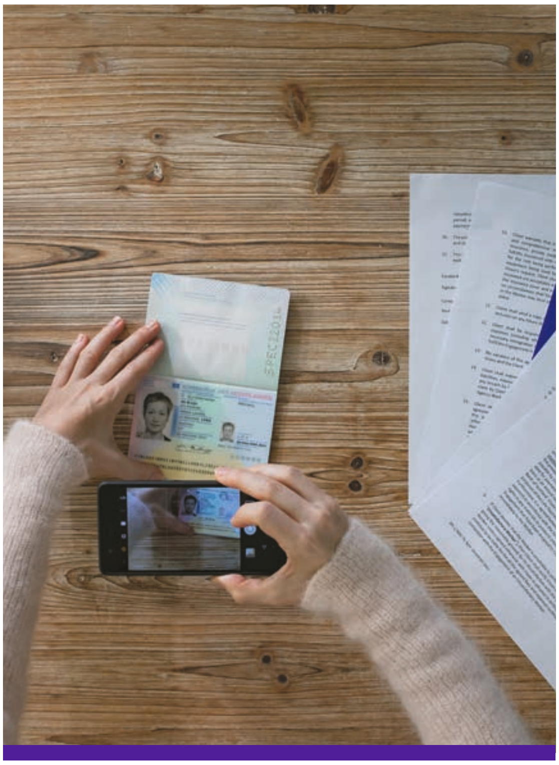
- Have a large customer base
- Are trusted by customers
- Have a deep expertise and experience in regulations (Know Your Customer, Anti-Money Laundering), data protection and privacy
- Manage a lot of customer data and can access and aggregate even more from readily available authoritative sources with IDEMIA Identity Platform

For example, mobile operators have access to various mobile device data including roaming, SIM swapping, lost & stolen devices, and location data. By collaborating with banks or other service providers, they can help prevent SIM-swap fraud and malicious account takeover. Likewise, banks can leverage their deep customer insights (bank records, account activity, loan application over time, credit ratings...) to provide an enriched and trusted digital identity to third-parties, upon consent of end-users.

IDEMIA's Identity Platform enables service providers to create another revenue stream by leveraging Identity as a Service to relying parties through the integration of a single API.

Identity Proofing

The platform performs identity proofing and verification for enterprises that need to know, trust and verify the identities claimed by their customers. Proofing is done using document and biometric capture with dedicated hardware or end-users' smartphones. Biometric and document data is then extracted and verified against one another or against a trusted data source, such as a national database or system of records.



Key features

ID document capture & verification

Biometric capture & verification

including liveness detection and anti-spoofing features

Root of trust checks

against highly trusted databases maintained by governments and other public authorities (passport registries, motor vehicle data, lost/stolen documents database...)

AML/CFT compliance checks

- Sanctions lists
- Watch lists
- Criminal and terrorists lists
- Politically exposed persons lists[2]
- Biometrics screening

Third-party database checks

- Credit scoring
- Financial footprint
- Telco data information

Universal connector

ID document capture and verification

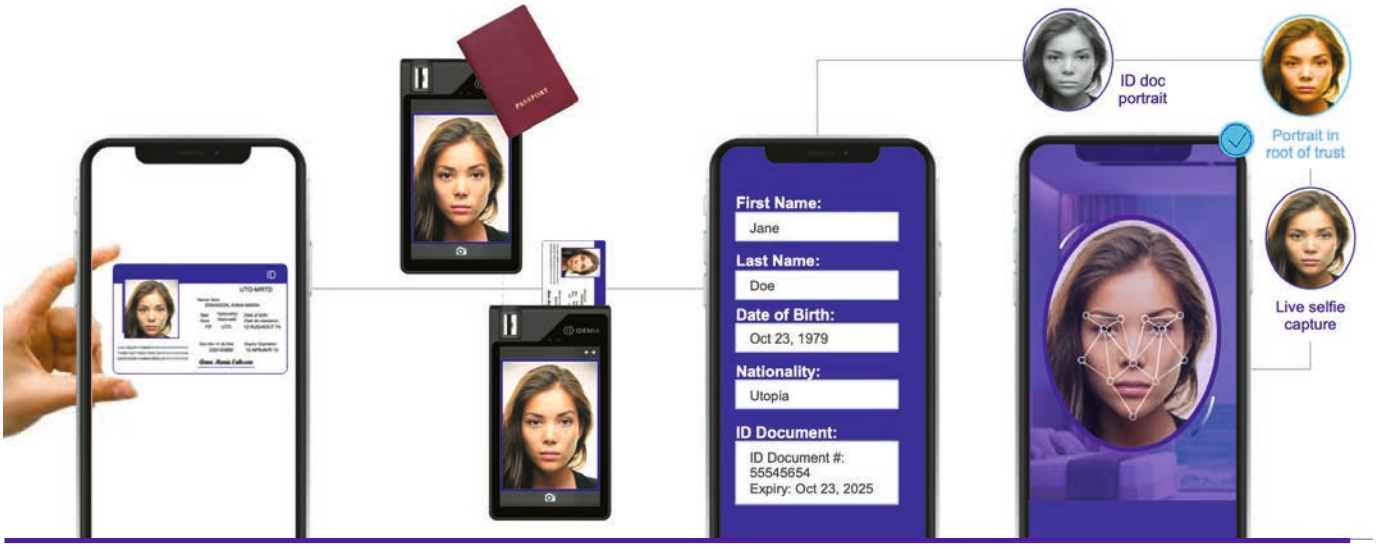
Identity Proofing is able to validate the authenticity of a wide range of ID documents from a large number of countries, including the detection of embedded security features and data to be extracted.

A set of mobile SDKs enables the capture of identity documents data either by taking a picture, reading the chip, or simply scanning and uploading a copy of the documents. MRZ (Machine Readable Zone) extraction and optical character recognition (OCR) can then be performed.

The capture can be done by the user with his mobile phone, or with the help of an agent, in-branch or in the field, via a tablet or a dedicated device, such as the ID Screen, exclusively developed by IDEMIA.

Digital Onboarding

Make user registration digital, safe and scalable



First Name: Jane

Last Name: Doe

Date of Birth: Oct 23, 1979

Nationality: Utopia

ID Document: ID Document #: 55545654 Expiry: Oct 23, 2025

Remote ID document capture

Customer scans ID doc using the smartphone camera. IDEMIA SDK captures and extracts the alphanumeric info and photo, and verifies the document's authenticity.

In-store ID document capture

Customer ID doc is captured in-store using IDEMIA's biometric-enhanced hardware terminals. MRZ and NFC chip reading methods of data extraction are both supported.

Automatic form filling

Extracted customer details are used to populate the registration form, reducing data entry errors and enabling a seamless user experience.

Subscriber matching with the ID document

Compare the portrait captured in ID document with the live selfie (and optionally with a root of trust) to provide the highest level of assurance.

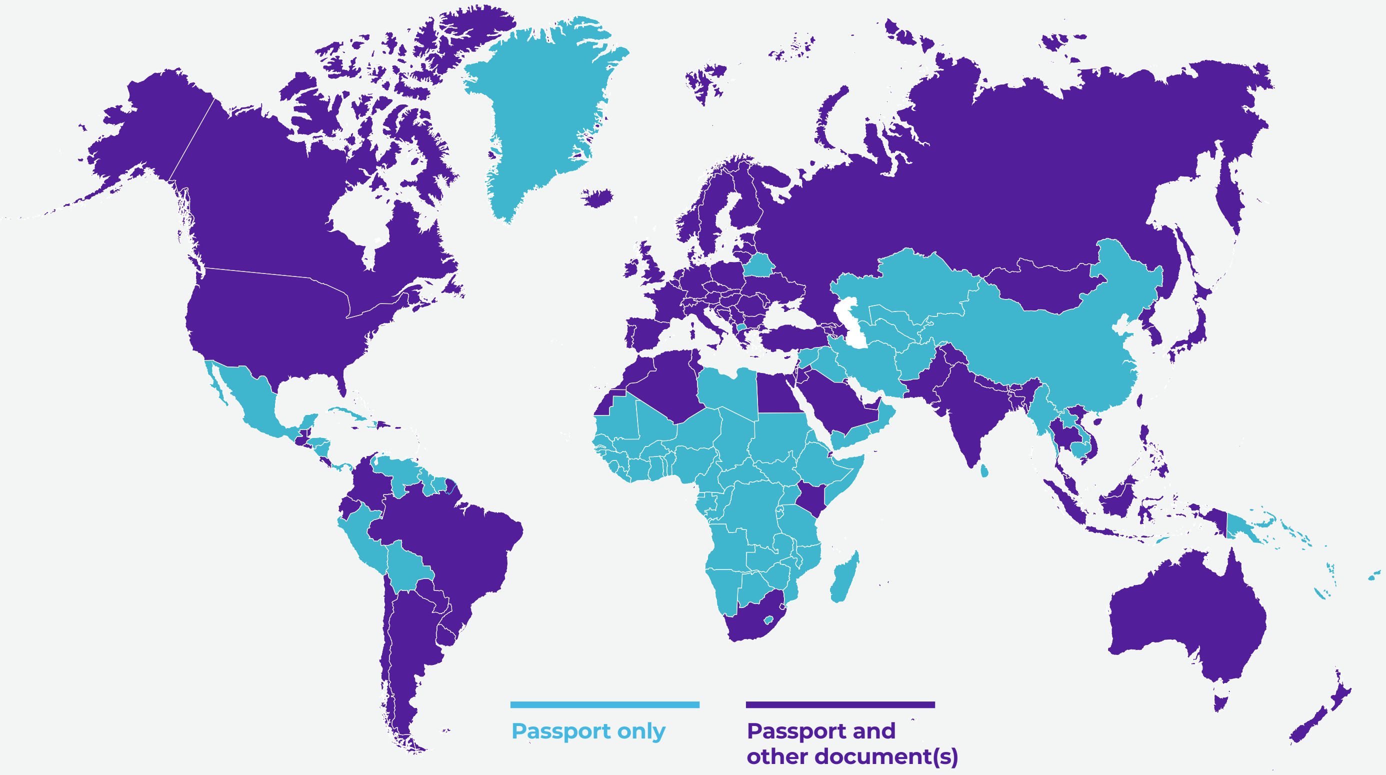
Identity Proofing performs

- consistency checks between the MRZ and the data extracted through OCR
- consistency checks of the data extracted from several documents and database
- detection and verification of the document's embedded security features

Supported documents

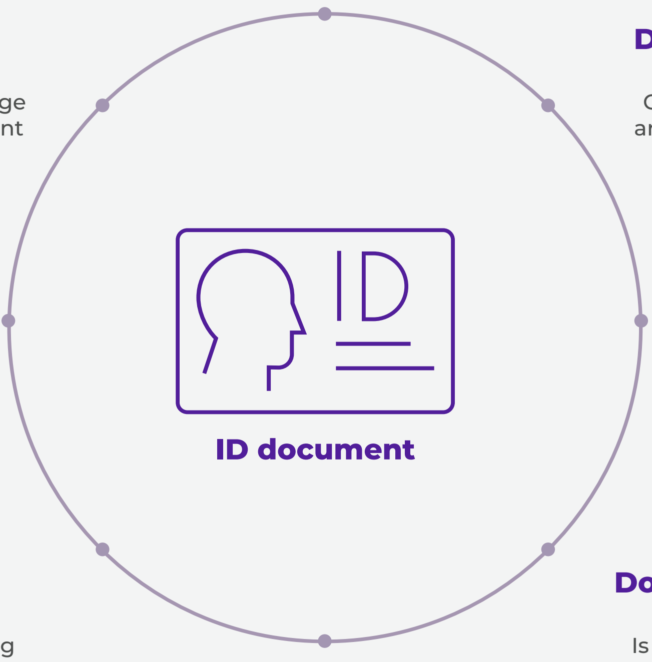
- ID card
- Passport
- Residence permit
- Driver's license
- Visa
- Immigration papers
- Voter identification document
- Tax identification documents and more

Over **4,500** different documents and passports for over **195** countries



Document verification

- Template
- Fonts
- Security features, including optically variable ink, holograms, fine line patterns, watermarks, stamps, optical stripe, security laminate...
- Text and barcode/MRZ consistency check
- Digital tampering
- Original document presence (no photocopy or screenshot)
- Known forgeries
- Image manipulation
- Pixel tampering
- Document to portrait check ...



Format/Template
Does the template match the expected template?

Digital tampering detection
Can we be sure that no areas have been digitally edited?

Font anomaly detection
Are all the fonts in this document consistent?

Document presence detection
Is this document actually present?

Checksum validation
Do the unique rules applied for generating fields match the expected outcome?

Data validation
Do the check sums flag any error in the data?

Field to field consistency
Does data remain the same across multiple sources in the document? Info in the MRZ consistent with info in the doc

Document identification
Identify submitted image as a known ID document type per library of templates

R O
O M

“Digital identity has the potential to unlock value by promoting inclusion, confidence, convenience and efficiency for both individuals and service providers.
It is the key to unlocking access to the global digital transformation now underway.”

Avneesh Prakash,
Head of Digital Identity, IDEMIA

Biometrics and liveness verification

Identity Proofing performs biometric matching and liveness detection of user biometric characteristics (face, fingerprints, etc.) against biometric information extracted from the ID document or from a reference database (root of trust), when available.

IDEMIA's SmartBio® and WebBioServer® SDKs both leverage the liveness detection technology, which enables clients to offer multi-channel identity verification solutions via Android and iOS mobile apps, or through web browsers on either desktop or mobile devices.

IDEMIA's liveness detection technology is available through the SmartBio® and WebBioServer® SDKs, and is part of the IDEMIA Identity Platform.

Root of trust verification

To provide the highest level of identity assurance and verify the claimed identity, Identity Proofing connects to highly trusted, external databases to perform checks. These external roots of trust can be maintained by governments, police, or other public authorities.

Root of trust sources

- National ID database
- Passport registry
- State or provincial motor vehicle office
- Public records
- Tax registry
- Any external ID document and/or biometric database

AML/CFT compliance and watchlist checks

To comply with the strictest Anti-Money Laundering (AML) and Counter Financing of Terrorism (CFT) regulations and obligations, Identity Proofing can screen an individual's information against external watch lists and check if a user exists on any known watch list maintained by governments, enforcement agencies, or financial authorities.

IDEMIA's Identity Platform can also perform biometric screening which offers compelling advantages over alphanumerical databases. If a high-risk individual attempts to enroll using a fraudulent identity document, the platform can identify them using only their biometric information.

AML/CFT compliance and watchlist checks

AML/CFT compliance watch lists	
International sanctions lists issued by EU[1], UN[2], OFAC[3], ...	**FATF lists** (Financial Action Task Force)
Country specific sanctions lists: Australia (DFAT[4]), UK (HMT[5]), France, Switzerland (SECO[6]), Netherland, Belgium, Singapore	**Custom watchlists** (provided by service provider, fuzzy search...)
Politically exposed persons (PEPs): politicians, judges, military, etc.	**Heads of international organizations, directors and major shareholder lists**
Law enforcement lists	**Criminal lists** issued by FBI, Interpol, etc.
Other watch lists (no-fly, sex offenders, etc.)	**Adverse media**

[1] European Union
[2] United Nations
[3] Office of Foreign Assets Control
[4] Department of Foreign Affairs and Trade
[5] Her Majesty Treasury
[6] State Secretariat for Economic Affairs

Third-party database and verification services

Relying on extensive and accurate data sources provides not only an opportunity to positively verify customer identity attributes, but also to enrich the digital identity with new elements.

Identity Proofing can be connected to third-party services to retrieve additional ID attributes and to cross-check the information that customers provide for verification and validation. Thus, the service provider benefits not only from its own data but also from data sets collected through multiple commercial touchpoints:

Banks	Bank records, account activity, loan applications over time
Mobile network operators	Roaming, SIM swapping, lost & stolen devices, location data...
Credit bureaus	Credit information and ratings platforms, such as Equifax, Experian, and TransUnion
Utilities service providers	Including telephone, gas, electricity or water

This enriched digital identity can be shared across a trusted network, upon consent of end-users. This capability is particularly valuable for Identity Providers aiming at providing an enhanced digital ID to other service providers.

Identity Proofing connects to external systems and databases, through a single API.

Identity Management

Once a customer identity is verified, Identity Management offers enterprises the ability to create, store and authenticate digital identities with a high level of security. Identity Management offers workflow management to perform ongoing biometric data deduplication, identity attribute enrichment and aggregation, compliance and watch list checks, manual adjudication services, and more, through the ID orchestrator and its universal connector API.

Identity lifecycle management

Updated and refreshed data is particularly useful in ensuring continued compliance with AML and KYC requirements. In fact, regulated professions are tasked with performing client due diligence on an ongoing basis throughout the lifetime of the client. Periodic client reviews also enable enterprises to heighten the Identity Assurance Level in order to provide more sensitive services such as life insurance.

Identity Management gives organizations full digital identity lifecycle management capabilities, which is key in maintaining the security and accuracy of digital identities, and in enriching them over time. Once data attributes have been collected and verified during onboarding, a digital identity is created and stored. It can be improved over time by collecting additional attributes, such as during KYC client review.

Key features

Identity lifecycle management

ID document database storage

Biometric database storage

Data deduplication

Case management for manual adjudication

ID orchestrator for workflow management

Universal connector

ID document database storage

The platform is able to insert, update and delete ID documents in a secure database so that the service provider can always rely on accurate and up-to-date ID document data throughout the identity lifecycle, notably to comply with KYC/AML regulations. It enables the service provider to provide up-to-date ID document for further verifications when needed, for instance in case of litigation. Transactions can also be validated by matching the submitted proofs against the stored ID document. The data is encrypted and securely stored according to the highest standards of security and privacy.

Biometric database storage

The platform is able to insert, update and delete biometric data in a secure database so that the service provider can always rely on accurate and up-to-date data throughout the identity lifecycle. Once the biometric attributes are created and stored, transactions can be verified against the database, providing an extra layer of security and assurance. Protection and privacy of biometrics are ensured throughout their lifecycle.

Data deduplication

Biometric deduplication involves a full database search for one or more candidates, based on their biometrics (also referred to as 1:N matching). It is essential in maintaining an identification system's reliability as it ensures that each person will have a unique identity. The process maintains a secure and sanitized database over time, as it can be applied to new or existing data.

Biometric deduplication is crucial in the fight against fraud and money laundering, enabling service providers to check whether a unique individual has opened multiple bank accounts under different or false names.

Biometric deduplication is also a very efficient way for service providers to maintain high data quality and to rely on a updated database, in order to maximize customer relationship management (CRM) scale and accuracy. That guarantees better performance and reliability, prevents data loss, data corruption and security breaches for an improved and more secure customer service.

Identity Management offers deduplication services to ensure a fully-fledged database sanity check. Depending on the use case, Identity Management is able to perform multi-modal biometrics search to accelerate the deduplication process and make it more accurate.

Attribute aggregation

Identity Management enables the enrichment of an identity by aggregating attributes from multiple sources, including third parties such as credit check companies or separate customer databases owned by the service provider. Identity Management creates a global user profile comprising all identity attributes and providing a 360-degree view of each digital identity for deeper customer insight. Better understanding of the customer enables advanced segmentation and personalized engagement, as well as modeling and analytics to refine service strategy.

This capability is particularly relevant for Identity Providers, allowing them to provide to other service providers an enriched digital ID of their common customers.

Manual adjudication

Identity Management provides a web based portal for human adjudication service to complement the automated verification process. It improves the conversion rates by processing transactions, which have been rejected automatically. It also provides an extra level of verification to enhance the identity assurance and to strengthen the security level, as individuals can be trained to spot certain things that systems may not.

Trained individuals connect to a secure, web-based portal and have access to the identity evidence necessary to perform a manual verification. In that portal, they can closely examine the submitted identity information (document, biometrics, etc.) and compare them against roots of trust or other available sources. This process can be done simultaneously with the other verifications, or at a later stage. IDEMIA can offer the full-service package or the individual software components for operation by the service provider.

ID orchestrator for dynamic workflow management

Identity Management includes an ID orchestrator which enables service providers to easily integrate, deploy and customize identity services depending on the local regulatory framework, business needs and the availability of data sources. A single API enables end-to-end workflow management for multiple channels and applications. It allows organizations to tap into internal and external sources for identity verification (compliance watch lists, root of trust, risk signals, and more).

The ID orchestrator is a web-based tool for customers to define their own identity workflows, including identity proofing, management, and authentication.

Identity Authentication

Identity Authentication enables organizations to verify the digital identity claimed by end-users so that they may access resources or perform online transactions whatever the channel: online, mobile, in-the field and in-store.

Our Identity Authentication solution allows companies to balance security and convenience, and comply with the latest regulations and standards regarding authentication: PSD2[1], 3D Secure 2.0 protocol and eIDAS[2] regulation. The stringency of authentication is adapted to the risk level of the transaction, with risk-based and multi-factor authentication. Thus, fraudsters are kept at bay, while legitimate users enjoy a frictionless authentication experience.

Multi-factor authentication

Multi-factor authentication (MFA) is a security measure that requires a user to provide at least two independent pieces of evidence to prove their identity.

KNOWLEDGE	**What users know** (password, PIN...)
POSSESSION	**What users own** (token, mobile, card...)
INHERENCE	**Who users are** (fingerprint,facial recognition, iris...)

[1] Payment Service Directive 2
[2] Electronic Identification and Trust Services

Key features

Two-factor authentication (2FA)

Multi-factor authentication

Biometric authentication

Transaction risk analysis

Risk-based authentication

It is also called strong authentication as it enhances the level of identity assurance, several factors being more difficult to falsify than just one. Multi-factor authentication is a key requirement of compliance with some regulations, such as the European Payment Service Directive 2 (PSD2), which demands that financial institutions implement strong customer authentication for sensitive transactions.

IDEMIA Identity Platform ensures multi-factor authentication. It supports a wide range of authentication factors and their combination:

- Mobile devices
- Multi-modal biometrics (fingerprint, face, voice...)
- SMS OTP
- OATH (Open AuTHentication)
- Software certificate
- Hardware certificate (certificate stored on a smartcard or token)
- Knowledge-based authentication (password)

Depending on the service provider's evolving needs, Identity Authentication can support new authentication factors at the lowest cost, with the simple integration of a plug-in, which allows:

The replacement or the complementing of a factor that has become vulnerable to attacks

The implementation of a new standard or authentication method

Two-factor authentication (2FA)

Identity Authentication supports two-factor authentication, which is a subset of multi-factor authentication. It only requires two pieces of evidence, while multi-factor authentication could involve additional pieces of evidence.

Biometric authentication

Biometric authentication relies on user's biometrics (face, fingerprint, iris) to verify their claimed identity, when logging to a service, an app or a device. For people on the move, it is easier than entering a complex password several times a day. It can also be used to control physical access points such as doors and gates.

Associated with a second factor of authentication, it offers a convenient yet secure customer experience. In particular, Identity Authentication proposes a Strong Customer Authentication (SCA) solution which combines mobile devices and biometrics and enables consumers to safely and conveniently transact online, in compliance with the PSD2 SCA requirements.

Transaction risk analysis

Identity Authentication is able to assess the risk level of a transaction by identifying and analyzing the context in which the user attempts to transact. It examines multiple contextual data points including the device, location, IP address, behavioral patterns, the nature of the transaction, and more.

By monitoring the context and risk of a transaction and comparing it with the user's transaction history, it can detect suspicious behaviors. If something is out of the ordinary, such as the login attempt is from a new machine or a new country, additional security steps are required and the user is prompted to authenticate. Highly suspicious and risky transactions can be blocked altogether.

Risk-based authentication or adaptive authentication

The platform ensures risk-based authentication, also called adaptive or dynamic authentication. It applies varying levels of stringency to authentication depending on the risk-level of the transaction, assessed through transaction risk analysis. As the level of risk increases, the authentication process becomes more comprehensive, demanding additional authentication factors. Identity Authentication enforces the authentication policy defined by the organization by prompting the user to authenticate with specified authentication factors depending on the risk-level.

In addition, the platform ensures adaptive authentication that embraces the hazards of daily life, such as when a user loses, breaks, or forgets the required authentication factors. In this case, Identity Authentication asks the user to provide an alternative method of authentication. This way, the user is not hindered from completing authentication and accessing the service, whilst the security level is preserved.

“A trusted digital identity has the power to transform KYC/AML compliance and fraud challenges into opportunities by enabling business growth, reducing costs, improving efficiency, and supporting the creation of new services.”

Muzaffar Khokhar,
EVP Digital Business Unit, IDEMIA

ABOUT IDEMIA

IDEMIA, the global leader in Augmented Identity, provides a trusted environment enabling citizens and consumers alike to perform their daily critical activities (such as pay, connect and travel), in the physical as well as digital space.
Securing our identity has become mission critical in the world we live in today. By standing for Augmented Identity, an identity that ensures privacy and trust and guarantees secure, authenticated and verifiable transactions, we reinvent the way we think, produce, use and protect one of our greatest assets – our identity – whether for individuals or for objects, whenever and wherever security matters. We provide Augmented Identity for international clients from Financial, Telecom, Identity, Public Security and IoT sectors.

With close to 15,000 employees around the world, IDEMIA serves clients in 180 countries.

We are **Digital**

idemia.com/**we-are-digital**

IDEMIA

Join us on

www.idemia.com