Identity Authentication
Adapt authentication to risk levels and use cases

A user-focused authentication solution that takes into account the context and the risk level of transactions is key to improve customer satisfaction, reduce fraud and meet regulations.

Embracing diversity

"Authentication" is the process of determining if users are whom they claim to be, by requiring them to provide pieces of evidence to prove their identity. It occurs each time a user attempts to access a service or perform a transaction.

Authentication factors can be categorized as:

› Inherence (fingerprint, face, iris, voice…)
› Possession (token, smartphone…)
› Knowledge (password, PIN…)

Other risk signals such as behaviorals (location, transaction history, device usage…) can be taken into account.

There is no "one size fits all" approach to authentication, in that it needs to take into account the:

› Business strategy
› Varying risk levels of transactions
› Variety of applications, channels and user profiles

› Evolution of fraud and rapid technological development
› Wide range of authentication factors available.

Identity Authentication

Our Identity Authentication Platform provides an adaptable platform capable of responding to the authentication needs of any service provider, regardless of the application, use case or channel. It enables adaptive authentication, adjusting the stringency of the authentication process to the level of transaction risk with:

› Multi-factor authentication
› Biometric authentication
› Transaction risk analysis
› Risk-based authentication

Identity Authentication is part of the IDEMIA Identity Platform, a universal platform for secure and trusted digital identity proofing, management and authentication.

Benefits

Convenience

› Adapt to user context
› Leverage mobile and biometrics for more security and convenience

Operations and profit optimization

› Create new value-added services for revenue streams
› Reduce fraud losses
› Improve efficiency in administering authentication

Trust and compliance

› Comply with latest regulations (PSD2 SCA[1], eIDAS[2], GDPR[3])
› Establish trust in transactions

Why IDEMIA?

› Global leader in biometrics with 40 years of experience in fingerprint, face and iris verification
› More than 3 billion identity documents produced worldwide
› Holistic approach to digital identity that is adaptable to local regulations and frameworks

⟨⟨|⟩⟩ IDEMIA

Adaptive authentication

Identity Authentication allows companies to balance security and convenience, and comply with the latest regulations and standards.


Multi-factor authentication

Supports a wide range of authentication factors:

› IDEMIA biometrics (ISO certified[4] liveness):
  - Mobile selfie
  - Web selfie
› OEM biometrics (iOS, Android)
› Device-bound keys
› Secure password
› SMS OTP
› Voice OTP
› MTLS[5] certificate
› OATH[6] hardware and software token
› FIDO2[7] WebAuthn

Biometric authentication

Proposes a Strong Customer Authentication (SCA) solution combining mobile devices and biometrics and complies with the PSD2 SCA requirements.
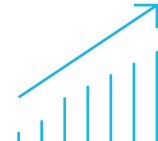
Risk-based authentication

Assesses the risk level by analyzing the transaction context (device, location, IP address, behavioral patterns, the nature of the transaction, and more) and applies varying levels of stringency to authentication depending on the risk-level.

Value proposition

Versatility and upgradeability
› Support of almost all factors
› Integration of new factors
› Independence from authentication factor suppliers

Global approach
› Multiple channels: web portals, mobile applications, in-branch, over the phone
› Multiple applications and use cases: online sales, online services, business applications

› Granular authentication policy implementation

User-friendliness
› SSO[8] authentication
› Fall-back method management

Easy administration and integration
› Provisioning and identity lifecycle management
› Factor lifecycle management
› Interoperability

IDEMIA Identity Platform

Identity Authentication is part of the IDEMIA Identity Platform. To learn more, visit idemia.com

› Identity Proofing
› Identity Management
› Identity Authentication

4: ISO-30107-3 level 1 & 2 certified liveness detection [Presentation Attack Detection] - 5: MTLS: Mutual Transport Layer Security - 6: OATH (Open AuTHentication) - 7: FIDO: Fast ID Online - 8: SSO: Single Sign On

IDEMIA

Join us on

www.idemia.com