WHITE PAPER

# Digital Identity for enterprises

A trusted digital identity is a powerful tool that is capable of securing access to essential services and expanding digital and financial inclusion.

IDEMIA

## Contents



# Augmented Identity

# Executive Summary

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. In this connected world, a secure digital identity enables people to safely access services and perform a wide range of transactions, from paying for their daily coffee to signing up for a new mobile line. This digital transformation has given individuals the ability to quickly and securely enroll and transact for public and private services alike.

Smartphones have played a significant role in the proliferation of digital identities. Cameras and fingerprint sensors can be used to capture physical identity credentials, selfies, and fingerprints which can then be verified against a trusted database. Forecasts indicate that by 2020, 100% of all smartphones shipped are expected to have biometric capabilities. Greater convenience and accessibility have helped to enhance the security of the ever-increasing number of digital transactions around the world.

Yet 1.1 billion people cannot officially prove their identity as they have no formal identification document or attribute on record. Moreover, about 3.4 billion people[2] have some form of identification, but are unable to use their identity online, thus making it more difficult for them to access critical public and private online services.

By instilling trust, ensuring privacy, and guaranteeing secure and authenticated transactions, digital identity has the power to unlock access to banking, payment, travel, communication and many other essential services. It is a powerful key to inclusive growth, creating value for all individuals and businesses.

[1] McKinsey & Company: Global payments 2018: A dynamic industry continues to break new ground

[2] McKinsey & Company: Digital ID: a key to inclusive growth

1.

# Augmented Identity as the genesis of trust

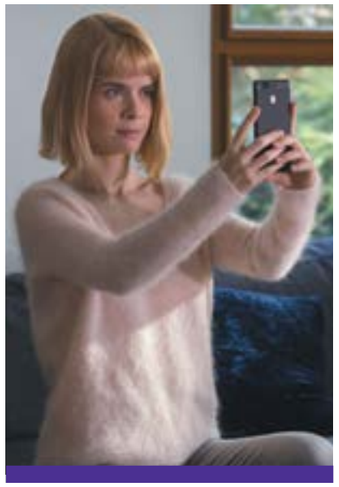
In the past, a trusted identity was easily established in face-to-face interactions using sight, names, and physical traits. As daily interactions increasingly move into cyberspace, there is friction in consumer journeys due to the systems and processes that were built primarily to handle physical identities. Likewise, governments and enterprises must update their legacy systems and infrastructure to enable the creation, storage, and use of digital identities. It is crucial that the same level of trust is replicated in the digital world.

## What is digital identity?

Digital identity is the online equivalent to the real identity of a person, entity, or object. It can be used to access, transact, and pay in the digital world.

A digital identity is comprised of multiple characteristics or identity attributes that can be physical features, such as a facial image or fingerprints, as well as personal data, such as name and date of birth.

Every person can possess multiple identities in the digital world by combining different attributes to respond to different use cases (opening a bank account, registering for a new SIM card, purchasing age-restricted items, etc.).



## What is Augmented Identity?

An Augmented Identity is an identity that ensures secure, authenticated, and verifiable transactions both in the physical and digital worlds.

An ideal Augmented Identity facilitates a smooth authentication and transaction process for individuals, while maintaining a high level of confidence.



Augmented Identity must promote:

| | |
|---|---|
| **Inclusiveness** | Anyone should be able to establish and use a digital identity to access services and assert rights, regardless of gender, age, ethnicity, religious background, etc. |
| **Security & privacy** | Identity data and transactions must be kept private, and must be protected from theft, unauthorized sharing, and unauthorized usage. |
| **Control & consent** | Individuals must be kept informed of the usage of their data and be able to choose what data they share, for which purpose, with whom, and for how long. |
| **Convenience** | It is easy to establish and use. |
| **Adaptability** | The amount and nature of identification data shared must be adapted to the use case. |
| **Wide acceptance** | It offers access to a wide range of useful services and interactions. |
| **Legal recognition** | To be truly effective, a digital identity must have legal recognition and protection. |

## Biometrics at the core of Augmented Identity

“Biometrics” refers to the use of the unique physical characteristics that identify an individual. Fingerprints, iris, voice and facial patterns all unique and accurate means of identifying individuals.

The use of biometrics is the single most effective contribution to Augmented Identity. It guarantees the uniqueness of an individual, and thus ensures that a person's identity can be trusted.

Biometrics is the assurance that only you can be you, and only you can prove it.

## The benefits of biometrics: combining security and convenience

### Biometrics as a means to combat identity theft

Unlike passwords, biometrics are the only means of establishing a link between physical and digital identities. This helps prevent identity theft, by enabling to prove that a person accessing an account or device is really who he or she claims to be. Besides, stealing biometric data without the person's knowledge, and then reproducing it in a useable form is not as easy as stealing a password and using it remotely.

### Biometrics: simpler than a password for authentication

Biometrics mean you no longer have to use unwieldy passwords. To be effective, a password has to meet four demanding criteria: it has to be changed frequently, be complex, it must vary from one account to another, and, above all, it must not be written down. For people on the move, biometric authentication is easier than entering a complex password several times a day.

### Biometrics make large-scale theft very difficult

While it's relatively easy to access thousands of accounts with stolen passwords in just a few seconds, it's much harder to hack biometric databases. In addition to gaining access to biometric data, thieves would also have to be able to produce fakes for each stolen element, and use them with the appropriate detector – thus eliminating the possibility of any large-scale attack. While the number of PIN codes is limited to the digits between 0000 and 9999, biometric data is unlimited.

2.

# Unlocking value with Augmented Identity

Digital identities can transform the future for billions of individuals all over the world, giving them access to new economic, political, and social opportunities, while ensuring digital safety, privacy and other basic rights.

The United Nations has identified 17 sustainable development goals to transform our world. These goals focus on several areas, but many can be greatly enhanced by the capabilities of secure digital identities. Moreover, the UN has also set a goal of providing everyone on the planet with a legal identity by 2030.

**Being able to prove one's identity is fundamental to an individual's ability to enforce their rights and secure access to a wide range of vital services such as mobile connectivity, healthcare, education, social protections and financial services.**

## Financial inclusion

Today nearly 1.7 billion adults worldwide, mainly in Africa, Asia, and Latin America, are still excluded from the formal financial system, not having any bank account or mobile money provider. This affects the most marginalized segments of society such as women, poor rural farmers, the elderly, persons with disabilities, and forcibly displaced people.

Although the causes of financial exclusion are many and varied, digital identity has the potential to remove some of the major barriers to the access and usage of financial accounts. By enabling people to prove their identity conveniently, it has the capacity to build trust, ensure ease of use, and lower costs, which are all essential to the wide adoption of financial services.

Using digital IDs to enable electronic Know-Your-Customer (e-KYC) and completely digitalize the onboarding process makes it easier for people to open an account and more affordable for financial service providers to reach underserved customers. This is especially true in rural and remote areas where it is not economically viable to set up a brick and mortar branch. According to McKinsey, e-KYC processes have the potential to reduce onboarding costs by up to 90 percent.

Access is pointless if people don't actually use the service. Globally, one-fifth of bank or mobile money accounts are inactive, without a deposit or withdrawal over the past year. As a World Economic Forum paper puts it: “Prosperity is not directly derived from the standalone ownership of bank accounts, but from their appropriate and consistent use.”

[3] World Bank blogs 3 Ways to advance usage and drive impact in financial inclusion

[4] World Economic Forum: Advancing Financial Inclusion Metrics: Shifting from access to economic empowerment



Convenience and confidence brought by smooth and intuitive authentication, using biometrics and mobile for instance, is key for boosting account usage, especially for people who may not be accustomed to using digital services.

Digital financial services and branchless banking services can be provided by many channels such as mobile phones, retail point of sales, other broadly available access points, and field agent banking. Thus, users can choose which channel is best suited for their needs. The ubiquity of mobile, in particular, represents a great opportunity in that matter, given that globally, about 1.1 billion remain unbanked, yet have a mobile phone.

The convenience of enjoying financial services at their doorstep is massive for people who sometimes have to travel long hours and lose a day of wages to reach a bank branch.

By achieving a critical mass of users and lowering operating costs with digital processes, the financial services provider is able to offer services at affordable prices.

## Accelerating the mobile money ecosystem

The prolific use of mobile in developing countries has given birth to financial innovations such as mobile money. Against a backdrop of increased connectivity and smartphone adoption, the use of mobile money has expanded the grid of financial services to include previously unbanked and underbanked populations.

Digital identity platforms provide 1.7 billion unbanked people with mobile phones with the ability to access secure financial services.

Agent networks play a key role in the success of mobile money services. Mobile money agents perform key tasks such as onboarding, over-the-counter transactions and supporting and educating customers. Furthermore, the presence of agents in hard-to-reach areas has been instrumental in financial inclusion.

[5] https://www.worldbank.org/en/news/press-release/2018/04/19/financial-inclusion-on-the-rise-but-gaps-remain-global-findex-database-shows [6] Source: GSMA Intelligence 2019

## Greater access to goods and services

Having a secure digital identity enables individuals to safely take advantage of the growing number of digital services provided by banks, telecom operators and retailers from the comfort of their home, or on the move. Unlike their brick & mortar equivalents, online stores and agencies are available 24/7. In addition to reducing costs for service providers and retailers, digital services translate into less time, hassle and cost for consumers.

## Access to employment and greater labor productivity

During the hiring process, job seekers are required to present their official documentation to the company so their academic and professional qualifications and achievements may be evaluated against the skills required.

Digital identity can help speed up the recruitment process by improving talent matching and background checks, automating identity verification, and enabling signature of contracts. It is particularly useful for the sharing economy, which depends on a mobile workforce to deliver products or services at customer doorsteps.

## Building trust and safety for the sharing economy

Sharing economies have turned out to be one of the fastest growing economies in the last decade, and the trend will continue as the world becomes more connected.

By 2025, the sharing industry is expected to reach global revenues of US$335 billion, an increase of 22.3% since it first emerged in 2014 as a $15 billion industry.

While convenience, economic value, and flexibility have driven the growth of sharing economies, the key to the growth of these new economies is a strong level of remote trust – a strong digital identity that is continuously authenticated remains a key engine of the sharing economy platforms, whether these are food-ordering services, ride sharing or car-pooling services. It builds confidence between all stakeholders: the companies that are providing services, the customers who are enjoying the services, the employees who are in the field, and the people who are lending their personal and valuable assets, such as their homes or cars.

[7] PwC https://www.pwc.com/us/en/technology/publications/assets/pwc-consumer-intelligence-series-the-sharing-economy.pdf



3.

# The benefits of digital identity

## Building trust

Digital trust is the foundation of all successful digital transformations. Digital identity is essential to establish an online model of trust that helps validate transactions and user identities reliably. It allows private and public entities to know with whom they are dealing, and, on the other side, it allows the consumers to know that they are dealing with a trusted party. As consumer and business confidence increases, the digital economy will expand. The example of the sharing economy, with online platforms connecting buyers and sellers, is particularly striking in this regard. Digital identity is able to establish trust between two strangers engaging online to transact sometimes very personal and valuable assets.

## Simplifying compliance and the burden of proof

The compliance burden for banks, payment companies, telecom operators, mobile money service providers and money transmitters is growing steadily with new and ever-stringent anti-money laundering (AML) and Know-Your-Customer (KYC) regulations. Banks are required to know who is opening an account. Similarly, in many countries, registration of prepaid mobile SIM cards is mandatory, requiring mobile operators to identify their customers when allocating or activating a SIM.

Increasing requirements are making the manual process more time-consuming, operationally demanding, expensive, inefficient and unreliable. As KYC processes become more complex, operational costs and fines for failure are increasing. Consult Hyperion estimates that KYC processes cost the average bank $60m annually.

Furthermore, lengthy onboarding processes (according to Thomson Reuters, it can take 48 days to onboard a new customer), can deter new customers from opening an account, resulting in financial losses.

Digital identity can help banks and financial service providers overcome the Know-Your-Customer hurdle by automating the identity verification process, with ID document authentication, biometrics and liveness detection checks, as well as Anti-Money Laundering (AML) and Combating the Financing of Terrorism database screenings. Digital Identity proofing, enhanced with Artificial Intelligence and Machine Learning capabilities, makes compliance processes more efficient, more reliable, cost-efficient and faster.

**Digital identities make it possible to reconcile compliance and the user experience. They enable eKYC, which enables enterprises to grow their customer bases using frictionless authentication and more customized services.**

## Reducing fraud

Fraud, implying massive data breaches and social engineering, costs companies billions of dollars. According to McKinsey, customer identity theft cost businesses an average of $148 per person from June 2017-June 2018.

As static personally identifiable information (PII) is likely to be stolen or compromised, businesses can no longer solely depend on this information to verify a user's identity. An efficient digital identity verification system enables them to adopt a dynamic approach, adapted to the risk-level of the transaction, that combines multiple data points from different up-to-date sources (ID documents, biometrics, behaviors, watchlists...). It enables them to better manage the risk of fraud, especially for remote transactions.

## Personalizing the customer experience

A digital service is not one-size-fits-all and has to be consumer-centric. Customers are looking for highly personalized and customized services, and the digital relationship must directly contribute to retaining their loyalty. Digital identity is key to building a standout, consistent and personalized customer experience across every channel, be it online, on mobile, via a call-center, in-store, or at the doorstep.



## Protecting privacy

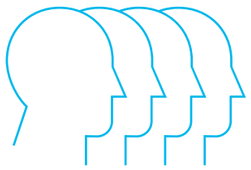
Regulations across the world, such as the European Union's General Data Protection Regulation (GDPR), the Asian-Pacific CBPR (Cross-Border Privacy Rules) or the California Consumer Privacy Act require effective privacy protections and give consumers control over their personal information.

In addition to data accuracy requirements, which demand collected data to be reliable and kept up-to-date, regulations set a “data minimalization” expectation. The collected personal data has to be adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed.

In other words, a well-designed digital identity system only discloses the credentials that are required for each specific service. For instance, for buying alcohol or playing online games, you only need to prove that you are old enough, but you don't have to reveal your name, address, and date of birth.

## Saving time and cost

Digital identity systems have the ability to save time and money for both organizations and consumers, as they streamline onboarding processes, signature of contracts and access to services. McKinsey estimates that customer onboarding costs could potentially be reduced by 90%, with delays reduced from several weeks to minutes. In remote and rural areas, it could also save people the hassle of traveling long hours to reach a bank branch, costing them a day of wages.



4.

# The digital identity value chain

Digital identity usage falls in two main use cases: identification and authentication.

"Identification" is the process through which we prove who we are. It establishes information about an individual using a set of attributes that uniquely describes him/her within a given context. It happens once in a while when we want to sign up to a new service like opening a bank account. "Identity proofing" is the validation of the claimed identity and attributes presented by the individual.

"Authentication" is the process through which we prove who we claim to be. It determines if one or several of the following elements or authenticators used to claim an identity are valid and belong to the same individual previously identified.

- What I have: mobile phone, smartcard, security token...
- What I am: fingerprints, face, iris...
- What I know: password, PIN code....

Authentication occurs each time a user wants to access a service.

**To ensure convenience and a true cross-channel experience, both the identification and authentication processes can be completed from several different locations including in-branch, online, in the field, or at a kiosk or ATM. In addition, consumers have both self-help and assisted options for enrolling, as well as for accessing services or making transactions.**

## Onboarding with identity proofing

For a service provider, a single category of verification is not sufficient enough to establish the legitimacy of an identity claim. A reliable digital identity requires a layered identity-proofing approach including ID documentation, biometrics, watchlists screening and third-party data, etc. It must also comply with local regulations. Organizations can pick and choose which of the layered measures to take based on their customers' profiles, their risk policy and identity assurance requirements. Such a multi-layered onboarding approach uses a combination of identity document authentication and biometric verification, AML/KYC watchlist screening, third-party verification and other background checks.




### ID Document Validation and Biometrics Verification

The identity document validation and biometrics verification process consists of extracting and verifying data from an ID document, authenticating the ID document and conducting a biometric facial check comparing a selfie of the customer with the facial image on their ID document. Verification may require a proof-of-life check to ensure the person behind the device is live and not a static image with liveness detection capability. In some cases, the fingerprint capture matching can happen against a database or a biometric template stored in a smartcard.

### AML/CFT Compliance and Watchlists Checks

To comply with the strictest Anti-Money Laundering (AML) and Counter Financing of Terrorism (CFT) regulations and obligations, in addition to identity document authentication and biometric checks, the digital identity system must screen an individual's information against PEP (Politically Exposed Person), criminals, terrorists and sanctions watchlists, to check if a user exists in any known watchlists maintained by governments, enforcement agencies, or public financial organizations.

### Third-Party Database and Verification Services

Relying on extensive and accurate data sources provides not only an opportunity to positively verify customer identity, but also to augment the digital identity with new attributes. Thus the digital identity system can also tap into a variety of trusted sources such as banks, credit bureaus, utilities service providers, mobile network operators, governments and public agencies, to cross-check the information that customers provide for verification and validation.

## Digital onboarding can occur through multiple channels:

### MOBILE ONBOARDING

enables consumers to enroll securely and digitally using their mobile devices, accelerating the opening of accounts. Users are guided to automatically capture documents and take a selfie using their mobile phones.

### ONLINE ONBOARDING

is a convenient and secure way for users to enroll using their PCs, with the ability to switch between devices. Biometric capture is made possible by built-in webcams and fingerprint sensors on supported devices.

### IN-BRANCH OR IN-STORE

allows agents to capture customer information including biometric data, ID document details and customer electronic signature using handheld devices for a complete digital in-branch or in-store enrollment experience.

### IN-FIELD ONBOARDING

enables agents to enroll consumers wherever they are, using a comprehensive solution including biometric hardware and software to capture and process data.

## Authentication to securely access, transact and pay

Authentication enables consumers to securely access, transact, and pay using self-help or assisted options. Typical use cases include checking balances, conducting money transfers, withdrawing and depositing cash, adding a beneficiary, applying for credit and making payments.

Balancing security with convenience is essential for authentication. Organizations must keep fraudsters at bay, while making the authentication process as easy as possible for legitimate users, providing them an excellent experience. This is made possible by implementing risk-based authentication, which adapts the stringency of authentication to the risk level of the transaction.

The risk-based authentication model identifies and analyzes the context in which the user attempts to transact, by examining multiple contextual data points including the device, location, IP address, behavior, the nature of the transaction and more. By monitoring the context and risk of a transaction, the company can detect suspicious behaviors. If something is out of the ordinary, such as a log-in attempt from a new machine, additional steps are required, and the user is prompted to authenticate, choosing from a wide range of factors, depending on the situation: multi-modal biometrics, mobile, SMS OTP, certificates, passwords, etc. Combining mobile and biometrics is particularly convenient to ensure a strong customer authentication so that consumers can safely transact online.

Furthermore, a well-designed digital identity system enables a consistent authentication experience for all channels: online, mobile, in-the field and in-store.

## Identity lifecycle management

Digital identities have to be managed throughout their lifetime in order for organizations to keep them secure and accurate, and to enrich them over time.

Once data attributes have been collected and verified during onboarding, a digital identity is created and stored. It can be expanded over time by collecting additional attributes. In addition to the KYC carried out at the time of account opening, the account holders may be required to undergo re-KYC and submit relevant information periodically. This keeps the company's records accurate and updated.

Deduplication offers a fully-fledged database sanity check because fake accounts are a major cause of money laundering. Biometric deduplication verifies whether a unique individual has opened multiple bank accounts under different names. The process maintains a secure and clean database to fight against fraud and money laundering.

Identity management also consists of performing the unbundling of identity, whereby only selected and necessary attributes are shared depending on the service accessed. Every combination of the data necessary for any given purpose is different. An identity management system that is respectful of privacy, should combine different required attributes or data depending on different contexts.

5.

# Digital identity in everyday life

Digital identities can be used across a growing variety of activities, services and industries. Online identity verification powers most of our everyday tasks, be it logging into apps, devices or services or transacting online. Financial services and insurance companies, retailers, telecom firms, gaming and retail are leading the adoption of digital identity.

**Financial services**

- Bank account opening
- Loan subscription
- e-contracting
- Online financial transactions (wire transfer, add new beneficiary, etc.)

**Telecom services**

- Prepaid and postpaid account opening
- Mobile money services
- Device swap
- IoT services

**eGov services**

- eVoting
- Tax payment
- Passport applications
- Benefits
- Driver's licenses
- Mobile identity

**Retail**

- Personalized online shopping experience
- Improved check-out

**Healthcare**

- Patient registration
- Patient data exchange
- Access to insurance services
- Improved medical treatment with shared data
- Qualification proofing of medical staff

**Sharing economy**

- Employee and customer onboarding
- Secure access to services



6.

# Digital identity as a new revenue stream

Organizations who are experienced in managing and protecting customer data are well positioned to provide value-added services to businesses looking to provide digital identity services for their customers. In doing so, and by enhancing their own offerings in parallel, these organizations can open up new revenue streams.

## Financial institutions and mobile operators are particularly well positioned to provide identity services:

- They possess an enormous amount of personal data due to the nature of their core business and a deep customer insight
- They are trusted by customers
- They have a large customer base that is attractive to relying parties and essential for critical mass
- They have extensive experience in validating and managing identities, both in the physical and the digital worlds
- They have expertise in compliance and risk-management having to abide by Customer Due Diligence (CDD), Anti-Money Laundering (AML) and Know-Your-Customer (KYC) requirements
- They are able to provide identities with a high level of assurance, as opening a bank account or registering a new SIM card requires a more reliable proof of identity than what a social network could offer

Mobile operators for instance, can leverage mobile device data, including roaming, SIM swapping, lost & stolen devices, and location data, to detect suspicious behaviors and fraud. They can, for example, help banks or other service providers to prevent SIM-swap fraud and malicious account takeover.

Likewise, banks can leverage their deep customer insight (bank records, account activity, loan application over time, credit ratings…) to provide an enriched and trusted digital identity to third-parties.

Thus, banks and mobile operators are able to generate new revenues from digital identity, not only by enhancing and extending their own offerings, but also by selling Identity-as-a-Service (IaaS) to adjacent service providers that cannot or do not wish to store and manage their clients' personal data.

7.

# It's more than a digital identity, it's a highway to digital freedom

At IDEMIA, the global leader in Augmented Identity, we work with institutions to enable millions of secured digital transactions.

IDEMIA is an established leader in identity and security solutions. For decades we have been trusted by governments to create physical identity documents such as passports, and our technology can be seen in the most secure areas of the globe.

Today we are on the cutting edge of digital identity technology. Our knowledge and experience ensure we lead the way with biometrics, blockchain and AI-driven solutions that together form the basis of a powerful digital identity platform.

With our technical expertise and experience, we help our customers and partners become a trusted issuer of digital identities, giving them a clear advantage in their respective industries. IDEMIA's mission is to enable a trusted and secure digital identity for creating a frictionless, safe and secure environment. We are here to make the world digitally yours.



At IDEMIA, we leverage our 2,000-strong R&D resources to enable a seamless transition to this digital world, working to create a trusted digital identity for everyone.

We have brought together complementary know-how and technologies that have never been combined before for both the physical and digital era: secured connectivity, secured payments and secured identity management. Not only does our technology help consumers and citizens alike travel with passports and pay with smartphones – it helps them identify themselves securely and effortlessly. With every technological disruption, we adapt to meet the new and evolving security demands of today and tomorrow.

In designing our market-leading solutions, we rely on the most unique, natural and authentic verification: the body's own biometric data. Your identity can be verified with a simple glance or the tap of a finger – which means that your identity cannot be stolen, imitated, jeopardized or corrupted. You are in direct control of your personal information.

IDEMIA's solutions are designed and deployed in accordance with local regulations, data privacy policies, business requirements, and more. This has been proven though multiple use cases in the field and our solutions are highly scalable, having been deployed in large-scale projects worldwide.

# 8.
# 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, travel and vote), 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 15,000 employees around the world, IDEMIA serves clients in 180 countries.

For more information, visit www.idemia.com / Follow @IdemiaGroup on Twitter

For more on digital identity
and our digital solutions, go to
idemia.com/we-are-digital

# We are **Digital**

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