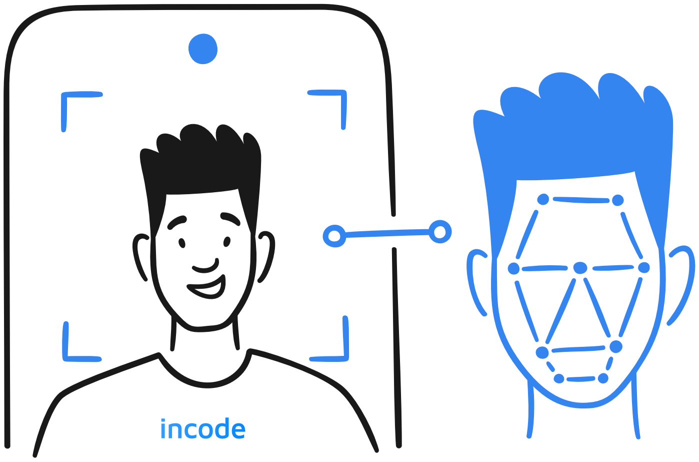
Biometric Technology: 7 Step Guide to Overcoming Common Misconceptions

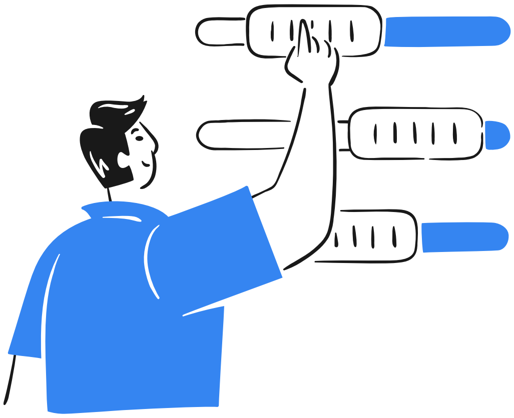
incode



Identity verification and affirmation technologies are having a transformative impact across business. With nearly $42 billion USD spent on identity verification alone, it's a fast expanding segment with almost limitless use cases ranging from its ability to improve relationships with customers, introduce new customer-friendly workflows, streamline on-boarding, improve regulatory compliance and guarantee personal data privacy.

Any discussion of biometric technology in a modern business context needs to align with a deeper understanding of its business value to the enterprise, and in particular, how different underlying approaches to biometric technology lead to varying levels of business outcomes. While early implementations of biometrics galvanized high levels of interest and introduced new and novel use cases, today's business requires orders of magnitude improvements in biometric performance, security, compliance and privacy for it to fully realize the potential of digital transformation at scale. Early adopters of biometrics often experienced the impact of poorly designed biometric architectures which lacked the full solution set of capabilities required for highly customized and industry-specific use cases, each with their own unique identity requirements. More often than not, poorly designed and incomplete identity offerings actually increase customer friction, create internal management challenges and increase corporate risk exposure.

This document outlines the key requirements for today's modern enterprise to successfully deploy biometric identity across their enterprise environment for optimal business results. It will consider various architectural approaches and product capabilities, offering practical insight on how to evaluate comparable solution sets in the context of supporting innovative digital transformation initiatives across industry-specific use cases.



Background and Immediate Benefits

The first record of a biometric identification system goes back to the 1800s in Paris, France, when Alphonse Bertillon developed a method of body measurements for the classification and comparison of individuals. While it looks entirely different today, its roots exemplify biometrics at its core: the ability to measure human traits or characteristics.

Today, biometrics technologies are widespread and form the basis of the Identity Proofing and Affirmation market, with applications that vary across almost all industries from finance to consumer goods, to hospitality and travel and entertainment to logistics, among many others. As such, biometrics are largely defined by the process of “confirming” a user is who they say they are against an actual certified “identity” record or document. The process compares an in-person user with a government-issued ID document, such as a passport or driver’s license.

Identity verification is a foundational element of advanced digital transformation, and has been accelerated by the need for remote and digital access due to the COVID-19 pandemic. The digital version of this process typically involves comparing a photo “selfie” or video with the government-issued document.

Digital identity proofing can greatly improve the accuracy of the verification process and speed the onboarding processes for almost all industries. Examples abound and include using face capture when opening a new bank account, contact-less check-in with a biometric kiosk at a hotel, or age verification for compliance at entertainment venues. When implemented correctly and with the right integrated set of capabilities, digital identity proofing results in higher accuracy/lower false positives, a greatly improved user experience and faster on-boarding, along with new types of use cases that increase customer engagement. What’s more, biometric technology is transforming how people interact across society. Some examples include:

Turning technology against human traffickers

Biometric techniques are useful for identifying victims and corroborating who knows whom to help investigate criminal cases and accelerate justice.

A new era of border security

Technological advances in biometrics hold the key to unlocking safer, more efficient US border operations

The move toward a cashless society

Biometrics is transforming the online and in-person shopping experience as retailers move to contactless cards and digital wallets process payments for everyday purchases.

With so many biometric identity solutions on the market today, ranging from physical to behavioral biometrics, it's often challenging to know which type of biometric solution, with which capabilities, fits a particular industry use case or application. For example, should active liveness, passive liveness or both be considered key required functionality. What flows should be considered critical and others "nice-to-have"? Another is balancing the need for accuracy with the need to maintain or improve customer retention and acquisition by ensuring speed and removing friction.

Without proper investigation and consideration many enterprises often struggle to deploy biometric verification seamlessly, and end up actually increasing corporate risk, slowing customer acquisition and adding extra management overhead complexities. Any organization looking to leverage biometrics to verify employees or end users should evaluate the underlying architectural platform and its integrated identity capabilities, as well as how their identification system is implemented, before they make their purchase decision.

Breaking Misconceptions – All Identities Are Not Created Equal

Despite a plethora of obvious business benefits, discrete examples have tainted the overall use of biometric technology in some cases. These examples should not only be treated as exceptions to the rule but serve as a playbook for how biometric technology should be implemented.

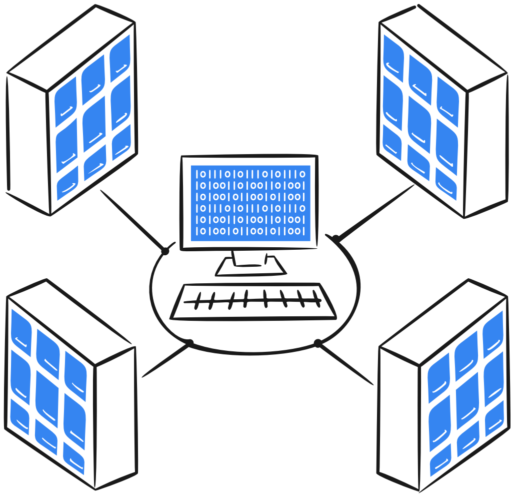
Eliminate Human Access to Data.

Using human or manual methods for identity verification is slow, inaccurate and exposes personal data to privacy issues. Even if manual methods are used infrequently in the solution, those cases are highly likely to result in a poor user experience with much longer verification times. By any measure, biometrics processes should be seamless and improve performance at least fivefold.

Best practices is a fully automated cloud-based AI platform that doesn't require manual, human-centric assessments in remote call centers operated by contractors. With advancements in machine learning, today's technology not only enhances the speed and accuracy of verified Trust, but also eliminates privacy abuses that occur only when human analysts interact with personal and confidential identity data.

Don't Hoard Data.

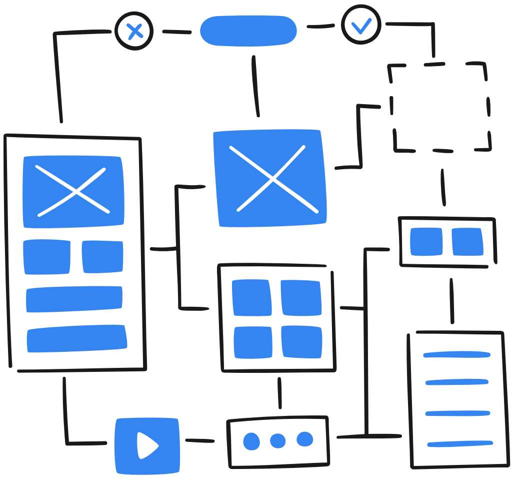
While biometric data is captured and matched against a verifiable and legitimate credential, storing it permanently should be avoided as much as possible, if not completely eliminated. If requirements exist to store information, storing data-at-rest should avoid plain text and be in a hashed or encrypted format. This is an important step to meet the compliance requirements for identity verification and authentication while preserving the privacy of the underlying data. These are most commonly found in decentralized identity architectures.



Eliminate Bias.

There is misconception is that machine learning is more biased that humans. However, research has shown that executed correctly, biometric technology in fact eliminates bias. Not only does it inherently begin as a blank slate, it has the ability to process a remarkable volume of diverse facial characteristics that the human brain could never keep pace with.

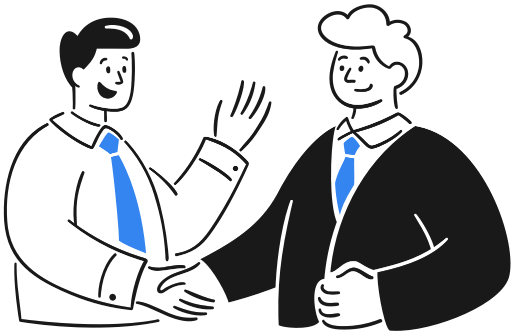
Foundationally, biometric bias is a result of homogenous training data; especially those based off of small sample sets. Algorithms learn using datasets. When datasets lean towards particular characteristics the machine learning model then focuses more on that particular characteristic. Known as over-fitting, this causes the system to be less able to identify alternate patterns. Therefore, the data is not actually biased towards a certain age or race, but less able to accurately identify the outlying demographics based on the original dataset.



Limit Data Handoff to 3rd Party OEMs.

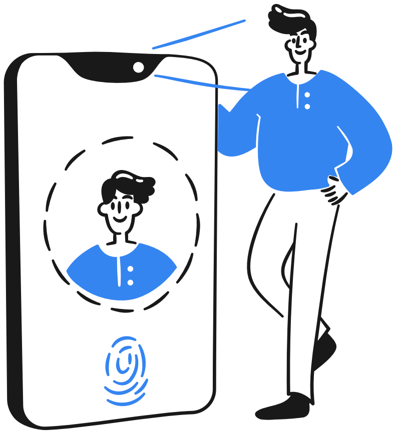
Rather than relying on an elaborate mix of disparate third party OEM technologies, biometric platforms should be purpose-built, fully-integrated modules that create seamless flows. This critical architectural approach not only guarantees pricing and product innovation, but it limits the movement of identity data. What's more, data is no longer stored, handled, or processed in various subcontracted vendor environments, environments that can not be audited or verifiably secured.

Leverage Government Partnerships.



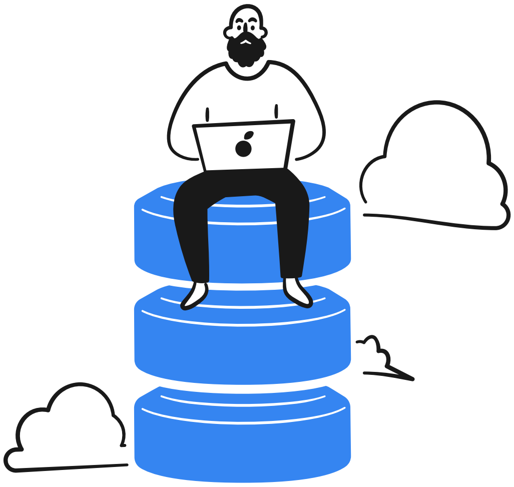
With a mandate focusing on expanding access to public resources for their citizens, national governments and state agencies are often pioneers in supporting the use of biometrics to verify and validate identities. These agencies play a leadership role in creating policies that securely regulate access to government-managed databases.

Through agreements with these government agencies, biometrics and identity verification solution vendors can remotely validate an identity without compromising the privacy or security of the underlying data or individuals. For example, instead of accessing the data directly, interactions are limited to a query string of quick and secure affirmative or negative responses (yes/no). The result is greater data privacy and security for both the agencies and their users.



Keep Processing at the Edge.

Biometrics, by definition, should be at the network edge and closest to the user. Not only is this best for privacy, but it increases responsiveness and speed. As much as possible biometric processing, including core artificial intelligence functions and biometric data processing should be done directly on the device. This delivers the low-latency performance required by today's businesses and limits the handling of identity information in off-premises infrastructure environments. There are multiple use cases, for example, where no Internet connection is a requirement for advanced biometric technology to function properly.



Deployment Options to Empower Flexible Controls.

Each organization is at its own stage of digital transformation, often a multi-year journey tackled in a phased approach internally and externally. Exemplified by the COVID-19 pandemic, external factors are increasingly forcing organizations to rapidly adapt to changing circumstances and adopt new, more flexible and remote digital processes. At the same time, compliance requirements are constantly evolving to protect user data.

For optimal flexibility and use case coverage, an identity proofing solution should be able to support every stage of an organization’s digital transformation journey. This means multiple deployment options including on-premises, SaaS, private cloud, or hybrid. Support for local compliance ordinances such as European data rules is also an advantage that allows the identity solution to scale seamlessly and adjust to the organization’s digital transformation needs while with flexible and highly customized identity flows that meet data residency requirements.